3/2015

Datenschutz Nachrichten

38. Jahrgang
ISSN 0137-7767
12,00 Euro

Douwe Korff

Peter Schaar

Peter Wedde

Thilo Weichert

Konferenz der Datenschutzbeauftragten des Bundes und der Länder

BvD e.V. Die Datenschützer

BfDI

FIfF

DIGITALE GESELLSCHAFT

DVD Deutsche Vereinigung für Datenschutz e.V.

digitalcourage

campact!.de DEMOKRATIE IN AKTION

GDD

verbraucherzentrale Bundesverband

Rote Linien zur EU-DSGVO

■ Europas Datenschutz ■ Wo sind die roten Linien? ■ Der Datengier gewidmet ■ Keine EU-Datenschutz-Grundverordnung ohne den Datenschutzbeauftragten ■ Europäischer Datenschutz: Bitte nicht aufweichen! ■ Zweckbindung revisited ■ Nachrichten ■ Rechtsprechung ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine



Freitag, 09. Oktober 2015
DVD-Vorstandssitzung
Bonn. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Freitag, 09. Oktober 2015 – Samstag, 10. Oktober 2015
DVD-Jahrestagung in Bonn
Thema: Unterwegs und überwacht
Informationen und Anmeldung:
https://www.datenschutzverein.de/jt2015

Sonntag, 11. Oktober 2015
DVD-Mitgliederversammlung in Bonn

Sonntag, 01. November 2015
Redaktionsschluss DANA 4/2015
Thema: Innere Sicherheit / Nachlese DVD-Jahrestagung

Foto: Uwe Schlick / pixelio.de

DANA
Datenschutz Nachrichten
ISSN 0137-7767
38. Jahrgang, Heft 3

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Jaqueline Rüdiger, Frank Spaeing
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße. 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@t-online.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0)91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 12 Euro. Jahresabonnement 42 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta, soweit nicht anders gekennzeichnet

Editorial

Liebe Leserin,
lieber Leser,

die Datenschutzrechte der EU-Bürgerinnen und -Bürger sind wieder einmal in Gefahr.

Es liegen die Entwürfe zur Europäischen Datenschutz-Grundverordnung (EU-DSGVO) der Kommission, des Parlaments und seit 15.06.2015 auch des Rates vor. Insbesondere letzterer Entwurf ist sehr verarbeitungsfreundlich. Am 24.06.2015 begann der sog. Trilog. Hierin versuchen Kommission, Parlament und Rat eine Einigung zu finden. Ende 2015 soll diese erzielt sein. Die Diskussionen zur EU-DSGVO standen von Vornherein unter übermäßigem Einfluss der Wirtschaftslobby. Es ist davon auszugehen, dass diese Einflussnahme während des Trilogs fortgesetzt und sogar noch verstärkt wird.

Nun besteht aus heutiger Sicht die vorerst letzte Chance, gegen erwartete negative Auswirkungen der EU-DSGVO zu intervenieren. Daher widmen wir uns dem Thema EU-DSGVO nunmehr mit dieser DANA erneut. Mit dieser Ausgabe soll ein umfassendes Stimmungsbild der im Datenschutz Aktiven entstehen. Wir hoffen, dass diese DANA denjenigen in Deutschland und in der EU, die Einfluss auf den Trilog nehmen können, Hilfestellung bietet.

In dieser Ausgabe führt uns zunächst Thilo Weichert in die Historie des europäischen Datenschutzes und der Vorschläge für eine EU-DSGVO ein. Dann äußern sich zivilgesellschaftliche Organisationen und Einzelpersonen, (Datenschutz-)Verbände, die BfDI sowie die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in kurzen Essays zu den Entwürfen der EU-DSGVO. Im Wesentlichen wird die Frage beantwortet, was die roten Linien sind, die beim Trilog in den kommenden Monaten nicht überschritten werden dürfen.

Auch der Europäische Datenschutzbeauftragte und der Evangelische Kirchentag haben sich mit der EU-DSGVO beschäftigt. Die entsprechende Pressemitteilung bzw. Resolution finden Sie im Anschluss an die Essays.
Des Weiteren liefert uns Jörg Pohle einen Aufsatz zum Thema Zweckbindung. Ein thematisch besonders zu dieser Ausgabe passender Aufsatz, da insbesondere nach dem Entwurf des Rates eine Aufweichung der Zweckbindung droht.
Außerdem finden Sie auf der Heftrückseite Informationen zu unserer im Oktober stattfindenden Jahrestagung „Unterwegs und überwacht – Mobilität, Telematik und Datenschutz“. Wir freuen uns über Ihre Anmeldung!

Nun wünschen wir Ihnen eine aufschlussreiche und kurzweilige Lektüre!
Jaqueline Rüdiger und Frank Spaeing

Autorinnen und Autoren dieser Ausgabe:

Jörg Pohle

studierte Rechtswissenschaft, Politikwissenschaft und Informatik. Derzeit promoviert er an der Humboldt-Universität zu Berlin zur Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung und koordiniert am Alexander von Humboldt Institut für Internet und Gesellschaft ein interdisziplinäres Forschungsprojekt zu Fragen der globalen Aushandlung im Privacy- und Datenschutzbereich (http://www.hiig.de/project/privacy-governance/).

Dr. Thilo Weichert

Ehemaliger Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein, Kiel, weichert@datenschutzzentrum.de

Thilo Weichert

Europas Datenschutz

Auf dem Weg zu einer Europäischen Datenschutz-Grundverordnung

Mit der Europäischen Datenschutz-Grundverordnung (EU-DSGVO) schafft die Europäische Union (EU) weltweit erstmals eine umfassend direkt anwendbare supranationale Datenschutzregelung. Sie wird zu einer wichtigen Grundlage für die Diskussion des Datenschutzes in einer globalisierten Informationsgesellschaft, die eine Strahlkraft und eine direkte Wirkung weit über Europa hinaus erlangen kann.

1. Europarat

Institutionelle Keimzelle des Datenschutzes in Europa war nicht die EU, sondern der Europarat, eine zwischenstaatliche Organisation mit Sitz in Straßburg, der u. a. auch Russland und die Türkei angehören. Nachdem in einigen industrialisierten Staaten in den 70er Jahren, allen voran in Deutschland, angesichts der Automation in Verwaltung und Wirtschaft, nationale oder regionale Datenschutzgesetze erlassen worden waren (im deutschen Bundesland Hessen trat 1970 weltweit das erste Datenschutzgesetz in Kraft), zeigte sich die Notwendigkeit einer überstaatlichen Regulierung: Datenschutz droht angesichts des globalen Handels entweder unwirksam oder ein Handelshindernis zu sein, wenn keine internationalen Standards festgelegt werden, bei deren Beachtung der grenzüberschreitende Austausch personenbezogener Daten erlaubt wird.

Mit dem *Übereinkommen Nr. 108* „zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten“ vom 28.01.1981 schuf der Europarat unter Verwendung der auf nationaler Ebene entwickelten Grundprinzipien allgemein anerkannte Mindeststandards für den öffentlichen wie für den privaten Bereich. In der Folge erarbeitete der Europarat eine Vielzahl von bereichsspezifischen Datenschutzempfehlungen, so etwa für folgende Bereiche: automatisierte medizinische Datenbanken (1981), wissenschaftliche Forschung und Statistik (1983), Direktwerbung (1985), soziale Sicherheit (1986), Polizei (1987), Arbeitsverhältnis (1989), Zahlungsverkehr (1990), Übermittlung durch öffentliche Stellen (1991), Telekommunikation (1995), Medizin (1997), Internet (1999).[1] Das Übereinkommen Nr. 108 wurde im Jahr 2001 mit einem Zusatzprotokoll zu Kontrollstellen und zum grenzüberschreitenden Datenaustausch ergänzt.

Für die Entwicklung des Datenschutzes in Europa war die Rechtsprechung des *Europäischen Gerichtshofes für Menschenrechte* (EGMR) mit Sitz in Straßburg von Bedeutung. Dieser kann angerufen werden, wenn in Mitgliedstaaten des Europarats Verstöße gegen die *Europäische Menschenrechtskonvention* (EMRK) geltend gemacht werden. Art. 8 der EMRK regelt:

Recht auf Achtung des Privat- und Familienlebens

(1) Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.

(2) Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.

Die Institutionen nach der EMRK in Straßburg erkennen immer mehr Teilaspekte des Datenschutzes als in den Schutzbereich des Rechts auf Privatleben fallend an. Der EGMR urteilte, dass selbst bei öffentlich frei zugänglichen Daten durch eine systematische Sammlung und Speicherung unzulässig in das Grundrecht nach Art. 8 eingegriffen werden kann.[2] Auch wenn vom EGMR noch kein eigenständiges Recht auf informationelle Selbstbestimmung anerkannt wurde, so kommt dessen Auslegung des Art. 8 EMRK einem modernen Verständnis von Datenschutz sehr nah.[3]

2. Der grundrechtliche Ansatz

Rechtlich hat Datenschutz in Europa zwei historische Ableitungen. Dies ist zum einen der Schutz der Privatsphäre, zum anderen der weiterreichende Schutz des allgemeinen Persönlichkeitsrechts. Während der erstgenannte Ansatz sphärenbezogen das Verhältnis zwischen Individualität und Gesellschaft einhegt, verfolgt der zweitgenannte Ansatz die Entfaltung individueller Freiheitsrechte, allen voran die allgemeine Handlungsfreiheit.

Diesem zweiten Ansatz verpflichtet entschied das *deutsche Bundesverfassungsgericht* (BVerfG) im Volkszählungsurteil vom 15.12.1983, dass jedem Einzelnen ein „*Recht auf informationelle Selbstbestimmung*“ zusteht, dem dieses Gericht wenig später explizit einen eigenständigen Grundrechtsstatus beimaß. Dabei beschränkte sich das BVerfG nicht darauf, dieses Grundrecht als subjektives Recht der einzelnen Menschen auszugestalten, sondern betonte dessen Rolle als „elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens“.[4] Diese Rechtsprechung wurde vom BVerfG weitergeführt, als es feststellte: „Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden

darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland".[5] Die Rechtsprechung des BVerfG entfaltete eine nachhaltige Wirkung auf die Rechtsprechung des EGMR, der nationalen Gerichte europäischer Staaten wie auch des Europäischen Gerichtshofes (EuGH), der obersten judikativen Instanz in der EU.

Der *EuGH* entwickelte sich nach vorsichtigen Anfängen immer mehr zu einer zentralen Quelle des europäischen Datenschutzes. In einem seiner ersten Urteile zu den gemeinsamen Gemeinschaftsgrundrechten erkannte der EuGH ein Recht auf Privatleben an.[6] Inzwischen gewährt er umfassenden Grundrechtsschutz bei der Verarbeitung personenbezogener Daten ohne Beschränkung auf sensible Daten oder eine direkte Beeinträchtigung beim Betroffenen. Parallel zur Entwicklung der Europäischen Wirtschaftsgemeinschaft zu einer Werteunion verlangte der EuGH für den Schutz personenbezogener Daten keinen Bezug mehr zu einer kommerziellen Tätigkeit. In seinem Urteil zur Vorratsdatenspeicherung vom 08.04.2014 bekräftigte der EuGH für die Verarbeitung personenbezogener Daten nicht nur die strenge Anwendung des Erforderlichkeits- und Verhältnismäßigkeitsgrundsatzes, sondern bestätigte die zuvor schon vom BVerfG in seiner Volkszählungsentscheidung begründeten Grundrechtsschutzprinzipen der Bestimmtheit und der Transparenz, der technisch-organisatorischen und der prozeduralen Sicherungen.[7]

3. Die Europäische Datenschutz-Richtlinie

Innerhalb der EU erwies sich schnell, dass der Rahmen der Europarats-Konvention Nr. 108 für die Entwicklung des europäischen Binnenmarktes nicht ausreicht und dass hinsichtlich des Datenschutzes eine höhere normative Verbindlichkeit nötig ist. 1975, 1976, 1979 und 1982 forderte das Europäische Parlament nachdrücklich eine verbindliche Festlegung der wichtigsten Verarbeitungsgrundsätze.[8] 1990 ergriff die Kommission dann endlich die Initiative und legte ein Bündel von Vorschlägen vor. Die Vorlage erschien dringlich, da 5 Mitgliedstaaten bis dahin immer noch keine Datenschutzvorschriften vorweisen konnten und dies die Vollendung des Gemeinsamen Marktes behinderte. Die Diskussion in den europäischen Gremien führte zu einer Übernahme von Regelungselementen aus verschiedenen nationalen Gesetzen und schließlich zur Verabschiedung der Richtlinie 95/46/EG „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" vom 24.10.1995 (*Europäische Datenschutzrichtlinie* – EG-DSRl). Wie schon der Titel erkennen lässt, soll diese Richtlinie im Rahmen des gemeinsamen Binnenmarktes den freien Datenverkehr innerhalb der EU gewährleisten. Ihr Anwendungsbereich erstreckt sich auf den öffentlichen wie auch den privaten Bereich, erfasst jedoch nicht den Polizei- und Justizbereich und auch nicht die gemeinsame Außen- und Sicherheitspolitik.

In Art. 29 EG-DSRl ist eine Arbeitsgruppe der Datenschutzbehörden der Mitgliedstaaten vorgesehen, der inzwischen auch der Europäische Datenschutzbeauftragte (European Data Protection Supervisor – EDPS) angehört. Der EDPS nahm 2004 seine Arbeit auf, nachdem die EU im Jahr 2000 in der Verordnung (EG) Nr. 45/2001 den Umgang mit personenbezogenen Daten durch die EU-Organe und dessen Kontrolle durch den EDPS geregelt hatte. Eine Funktion des EDPS besteht darin, die EU-Kommission zu beraten, soweit deren Aktivitäten Auswirkungen auf den Datenschutz haben. Die *Artikel-29-Arbeitsgruppe* koordiniert die Arbeit der nationalen Datenschutzbehörden in der EU, um unter Anwendung der gemeinsamen europäischen Regelungen ein einheitliches Datenschutzniveau zu gewährleisten.

Neben der EG-DSRl erließ die EU inzwischen eine Vielzahl weiterer Regelungen, die explizit oder indirekt Relevanz für den Datenschutz haben. Von besonderer Bedeutung ist insbesondere die *Datenschutzrichtlinie für den Bereich der Telekommunikation*.[9] Diese Richtlinie zur elektronischen Kommunikation wurde 2009 überarbeitet und sieht seitdem z. B. vor, dass Verletzungen des Schutzes personenbezogener Daten gemeldet werden müssen.[10] Mit einer weiteren Richtlinie wurden die EU-Mitgliedstaaten zu Regelungen verpflichtet, eine Speicherung von Verkehrs- und Standortdaten der elektronischen Kommunikation für Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten sicherstellen.[11] Diese Richtlinie wurde vom EuGH mit Urteil vom 08.04.2014 wegen Verletzung der Grundrechte auf Privatsphäre und auf Datenschutz aufgehoben.[12]

In Anwendung der EG-DSRl präzisierte der *EuGH* die Anforderungen an die personenbezogene Datenverarbeitung in der EU. Mit den Urteilen vom 09.03.2010 und vom 16.10.2012 betonte das Gericht die Notwendigkeit der Unabhängigkeit der Datenschutzaufsichtsbehörden.[13] Mit Urteil vom 29.06.2010 entschied sich der EuGH bei einem Konflikt zwischen Informationsfreiheit und Datenschutz zugunsten des individuellen Grundrechtsschutzes des von der Verarbeitung Betroffenen.[14] Mit Urteil vom 24.11.2011 stellte der EuGH klar, dass die verpflichtenden Regelungen der EG-DSRl es verbieten, dass die nationalen Gesetzgeber nach oben wie nach unten hiervon abweichen (sog. Vollharmonisierung).[15] Mit Urteil vom 13.05.2014 wurde die umfassende Anwendbarkeit der EG-DSRl für Internetsuchmaschinen bestätigt und die datenschutzrechtlichen Anforderungen einer differenzierten Interessenbewertung bei der Sperrung/Löschung von Daten präzisiert.[16] Mit Urteil vom 11.12.2014 stellte der EuGH klar, dass die EG-DSRl bei einer Erfassung des öffentlichen Raums (hier Videoüberwachung) anwendbar ist und die Privilegierung für ausschließlich persönliche und familiäre Tätigkeiten nicht gilt.[17]

Die *polizeiliche und justizielle Zusammenarbeit* in der EU, die frühere „dritte Säule" des EU-Vertrags, ist bisher weitgehend unreguliert und blieb so ein Flickenteppich einiger europäischer, vieler nationaler und teilweise – wie in Deutschland – regionaler Regelungen. Für alle EU-Mitgliedstaaten gilt das Übereinkommen Nr. 108 des Europarats. Vom Europarat stammt zudem eine Empfehlung zum Datenschutz im Polizeibereich.[18] Viele Mitgliedstaaten haben sich dafür entschieden, den Polizei- und Justizbereich in den Umsetzungsakt der Richtlinie 95/46/EG mit einzubeziehen. Zu Europol, Eurojust,

zum Schengener Informationssystem sowie zur Flüchtlings- und Ausländerpolitik gibt es spezifische Datenschutzregelungen auf EU-Ebene. Schließlich gibt es bzgl. des Informationsaustauschs zwischen den Mitgliedstaaten einen Rahmenbeschuss 2008/977/JI, der bis Ende 2010 national umgesetzt werden musste, aber nur ein niedriges Schutzniveau gewährt. Die EG-DSRl schließt den Polizei- und Justizbereich ausdrücklich aus. Entsprechendes gilt für die geplante EU-DSGVO. Für diesen Bereich ist eine eigenständige Richtlinie geplant, die sich jedoch noch nicht im Trilogverfahren befindet.

4. Europäische Grundrechtecharta

Lange war Datenschutz als Grundrecht durch den EuGH nur als gemeinsamer Standard der Mitgliedstaaten anerkannt. Dies änderte sich durch den am 01.12.2009 in Kraft getretenen Vertrag von Lissabon, zu dem eine „Charta der Grundrechte" (EUGRCh) gehört, über die man sich schon im Jahr 2000 verständigt hatte. Dort sind in den Art. 7 und 8 die Privatsphäre und der Datenschutz gewährleistet.

Artikel 7 – Achtung des Privat- und Familienlebens

Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.

Artikel 8 – Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Der Vertrag von Lissabon, mit dem die Säulenstruktur der EU beseitigt wird, sieht mit Art. 16 Vertrag über die Arbeitsweise der Europäischen Union (AEUV) eine allgemeine Datenschutzregelung vor, die das Europäische Parlament und den Rat der EU beauftragt, Vorschriften zum Datenschutz zu erlassen. Die Regelung begründet zugleich ein subjektives Recht auf Datenschutz, wobei unklar ist, inwieweit unter Berufung hierauf gerichtliche Klagen gestützt werden können.

5. Der Konflikt mit den USA

Die Diskussion um den Datenschutz in Europa steht in einem praktischen Spannungsverhältnis zu Bestrebungen und zur Rechtssituation in den USA: Dort ist bis heute vom obersten Gericht, dem US Supreme Court, kein Grundrecht auf informationelle Selbstbestimmung oder auf Datenschutz anerkannt. Zwar sieht der US Supreme Court sog. „chilling effects" durch informationelle Maßnahmen auf von der Verfassung geschützte Rechte wie Meinungs-, Presse-, Informations- und Versammlungsfreiheit. Auch sind materielle Auswirkungen informationeller Maßnahmen justiziabel. Doch personenbezogene Datenverarbeitung selbst wird als Grundrechtseingriff nicht akzeptiert. Grundrechte binden nach herrschendem US-Verständnis in keiner Weise private Unternehmen und gelten nur für US-Einwohnerinnen und -Einwohner, also z. B. nicht für die ausländische Kundenschaft von US-Internetunternehmen. Betroffenen werden allenfalls „*reasonable expectations of privacy*" zugestanden, wobei vernünftige Erwartungen an die Wahrung der Privatheit unvernünftig eng interpretiert werden. So besteht gemäß der „third party doctrine" kein Schutz bei Daten, die einmal auf Betreiben eines Betroffenen in den öffentlichen Raum gelangt sind. Sicherheitsbelange ebenso wie kommerzielle Verwertungsinteressen werden von der Rechtsprechung als grundsätzlich überwiegend gegenüber Interessen von Betroffenen auf informationellen Schutz bewertet. Dies ist zweifellos für die US-amerikanische Sicherheitsdominanz sowie für die Marktdominanz der dort beheimateten Unternehmen – von Amazon über Apple, eBay, Facebook, Google, Microsoft bis Salesforce und Uber – förderlich. Für die Wahrung der Datenschutzrechte der Menschen in Europa, die manchmal freiwillig, manchmal gezwungenermaßen die Dienstleistungen der US-Anbieter verwenden, ist dies jedoch fatal.

Anders als die Bundesregierung hat die *EU-Kommission* erkannt, dass die Missachtung des Datenschutzes durch US-Unternehmen die Wahrung des Grundrechtsschutzes in Europa generell untergräbt und dass dies zugleich zu einer Marktverzerrung zulasten europäischer Anbieter führt, die dem europäischen Datenschutzrecht effektiver unterworfen werden können. Dies führt z. B. dazu, dass der Safe-Harbor-Beschluss der EU-Kommission aus dem Jahr 2000 heute von dieser in Frage gestellt wird. Mit ihm sollte der freie Austausch mit US-Unternehmen und damit der wirtschaftliche Anschluss an die informationstechnische Entwicklung in den USA erreicht werden. Inzwischen hat Safe Harbor den entgegengesetzten Effekt und untergräbt zugleich die digitalen Grundrechte der Europäer. Die EU-Gremien sehen in der Vereinheitlichung und Effektivierung des Datenschutzes in Europa ein Instrument, um der ökonomischen US-Dominanz etwas rechtlich entgegen setzen zu können.[19]

Diese Herausforderung erkennend, versuchen die USA den Prozess der Vereinheitlichung und Effektivierung des Datenschutzes in Europa mit allen Mitteln zu bekämpfen. Dies äußert sich in intensiver *Lobbyarbeit* in Brüssel nicht nur durch private Einrichtungen, sondern auch durch die Obama-Administration. Dabei geht es nicht nur um die Verteidigung des Safe Harbor, sondern um direkte Einflussnahme auf die europäische Normsetzung sowie um den Versuch, über das Freihandelsabkommen TTIP zu einer Senkung der europäischen Datenschutzstandards zu kommen.[20]

6. Vorschläge zur EU-DSGVO

Schon vor dem Inkrafttreten des Vertrags von Lissabon 2009 hat die EU-Kommission eine offene Konsultation zur Überarbeitung der EG-DSRl gestartet. Im November 2010 veröffentlichte dann die Kommission eine Mitteilung über ein Gesamtkonzept für den Datenschutz in der EU. Darin wird als Ziel

vorgegeben, das Datenschutzrecht weitgehend zu harmonisieren, ein „Recht auf Vergessen“ zu etablieren, die Unabhängigkeit der Datenschutzbehörden zu verbessern und die Regelungen über den Datentransfer in Drittstaaten zu optimieren.[21]

Am 25.01.2012 legte die *EU-Kommission* einen umfassenden Vorschlag einer Europäischen Datenschutz-Grundverordnung (EU-DSGVO) vor. Dieser Vorschlag ist Teil eines größeren Pakets zur Reform des EU-Datenschutzrahmens, zu dem auch Richtlinien-Vorschläge für den Bereich der Strafverfolgung gehören. Die Kommission entschied sich nach langer Diskussion – anders als im Bereich Innen und Justiz – für das Instrument einer direkt anwendbaren Verordnung und gegen eine durch nationales Recht umzusetzende Richtlinie, um einen einheitlichen Rahmen für die Privatwirtschaft und weite Teile des öffentlichen Sektors zu erlangen.[22]

Die Argumente, die für eine einheitliche Regelung sprechen, sind erdrückend: Angesichts des informationstechnischen Binnenmarktes benötigen sämtliche Beteiligte, insbesondere die Unternehmen, einheitliche Datenschutzstandards, um nicht einem Regelungswirrwarr ausgesetzt zu sein, der nationales oder regional unterschiedliches Vorgehen nötig macht. Zudem ist es durch gemeinsame Regeln einfacher, sich gegen internationales Datenschutzdumping, komme es nun aus den USA oder aus Südostasien, zur Wehr zu setzen. Dessen ungeachtet gehörte die deutsche Politik lange Zeit zu den Kräften, die gemeinsam mit notorischen Datenschutzverweigerern in der EU wie Großbritannien und Irland das Zustandekommen der einheitlichen Regeln behinderte. Bereits am 30.03.2012 legte der deutsche Bundesrat eine Subsidiaritätsrüge ein mit der Begründung, es sei nicht ausreichend dargelegt, weshalb eine verbindliche Vollregelung auf europäischer Ebene erforderlich sei.[23]

Die EU-DSGVO soll eine umfassende direkt anwendbare Datenschutzregelung für ganz Europa sein, die mit technik- und zukunftsoffenen Regelungen größtmögliche Verbindlichkeit hat. Folgende Grundprinzipien werden dabei verfolgt:

- Die neuen Datenschutzregeln sollen auch für Anbieter gelten, deren Datenverarbeitung außerhalb der Union stattfindet, ihre Angebote aber an Menschen in der EU richten (wie etwa Facebook und Google).
- Bei internationalen Einrichtungen soll für die konkreten Kontroll- und Sanktionsmaßnahmen nur die Aufsichtsbehörde zuständig sein, die sich am Hauptsitz befindet (One-Stop-Shop). In einem Kohärenzverfahren werden andere beteiligte Aufsichtsbehörden eingebunden.
- Die Betroffenen müssen über den Umgang mit ihren Daten durch Transparenzregelungen und Auskunftsansprüche über Stellen, Zwecke und Speicherdauer informiert werden. In Internet-Datenschutzerklärungen sollen standardisierte Symbole verwendet werden.
- Durch datenschutzfreundliche Techniken und Grundeinstellungen (privacy by design und by default) sollen die verwendeten IT-Produkte die Umsetzung des Datenschutzes fördern.
- Die bisherige Vorabkontrolle wird zu einer Risiko- und Folgenabschätzung ausgebaut. Mit Zertifizierungsverfahren und Audits soll das Risiko von Datenschutzverstößen reduziert werden.
- Datenschutzpannen sind zeitnah gegenüber den Aufsichtsbehörden und den Betroffenen zu melden.
- Verbindliche interne Unternehmensrichtlinien (Binding Corporate Rules) sollen gestärkt werden.
- Die Beschwerde- und Rechtsschutzmöglichkeiten für die Betroffenen werden verbessert.
- Bei Datenschutzverstößen sollen deutlich höhere Bußgelder als derzeit verhängt werden.

Am 12.03.2014 beschloss das *Europäische Parlament* auf der Basis der Kommissionsvorschläge einen eigenen von dem grünen Berichterstatter Jan Phillipp Albrecht ausgehandelten Textvorschlag.[24] Von den 653 an der Abstimmung Beteiligten stimmten 621 dem Text zu, 10 Abgeordnete stimmten dagegen, 22 enthielten sich. Vorausgegangen war am 21.10.2013 eine entsprechende positive Entscheidung durch den Innen- und Justizausschuss des Parlaments (LIBE, 49 Ja-Stimmen, 1 Gegenstimme, 3 Enthaltungen).[25] Parallel beschloss das Parlament mit einer geringeren Mehrheit sein Votum zu einem Richtlinienvorschlag für den Polizeibereich. In dem zwei Jahre dauernden Verhandlungsprozess waren offiziell ca. 3000 Änderungsvorschläge erörtert worden, die teilweise direkt von Lobbygruppen über Parlamentarier in das Verfahren eingeführt worden waren. Im Ergebnis folgte der Parlamentsvorschlag weitgehend der Kommission. Er sieht jedoch einen geringeren Einfluss der Kommission und eine Stärkung der unabhängigen Datenschutzbehörden vor. Viele Änderungen enthalten inhaltliche wie prozedurale Präzisierungen und verbessern die Transparenz. Die Umsetzungsinstrumente werden geschärft, etwa durch eine Höchststrafe bei Datenschutzverstößen von 100 Mio. Euro oder 5% des Jahresumsatzes eines Unternehmens.

Die Diskussionen um die EU-DSGVO stehen von Anfang an unter massivem Lobbyeinfluss. Dieser Einfluss führte kurz vor der Veröffentlichung der Kommissionsvorschläge 2012 noch zu einer Veränderung in der Zustimmungsanforderung für die werbliche Datennutzung. Doch selbst die nun vorgesehenen sehr freizügigen Nutzungsregelungen sind weiterhin Gegenstand massiver Kritik von Wirtschaftslobbyisten hinter verschlossenen Türen.[26] Von Nichtregierungsorganisationen wurden auf dem Portal LobbyPlag.eu rund 11.000 Seiten an Dokumenten zu den Verhandlungen zusammengetragen und analysiert. Von den dabei untersuchten insgesamt 517 Anträgen zielten laut LobbyPlag 403 darauf ab, das ursprünglich anvisierte Datenschutzniveau abzusenken, nur 114 forderten eine rigidere Verordnung.[27]

Mit Datum vom 15.06.2015 einigten sich die Innen- und Justizminister im *Rat der EU* nach langen Verhandlungen auf ihre Positionen zur EU-DSGVO.[28] Noch unter dem *Bundesinnenminister* Hans-Peter Friedrich hatte die deutsche Delegation die Verhandlungen immer wieder dadurch behindert, dass sie nach außen hin die Position äußerte, das hohe deutsche Datenschutzniveau müsse erhalten bleiben. Ansatzpunkt der deutschen Kritik war die geplante einheitliche Anwendbarkeit der EU-DSGVO im öffentlichen wie im nicht-öffentlichen Bereich. Es wurde die Befürchtung geäußert, die ausdifferenzierten deutschen Regeln im öffentlichen Bereich müssten aufgeben werden. Zugleich machte

sich das Bundesinnenministerium zum Sprachrohr einer juristisch abseitig bleibenden Minderheitenposition, wonach im nicht-öffentlichen Bereich beim Datenschutz das Verbot mit Erlaubnisvorbehalt abgeschafft gehöre. Mit dieser Position wird seit Jahren versucht, Wirtschaftsunternehmen von strengen Datenschutzanforderungen zu befreien.[29] Unter Bundesinnenminister Thomas de Maizière wurde dann eine konstruktivere Verhandlungsstrategie verfolgt.

Die *Position des Rates* ist verarbeitungsfreundlicher als die der Kommission und erst recht des Parlaments. Anstelle einer „ausdrücklichen" Einwilligung soll diese nur „unzweideutig" sein. Zweckänderungen werden bei „berechtigten Interessen" erleichtert. Werbenutzungen sollen grds. nur durch Widerspruch verhindert werden können; Einwilligungen sind zumeist nicht gefordert. Das Prinzip der „Datensparsamkeit" spielt nur noch eine untergeordnete Rolle. Als Sanktionshöhe sind – erheblich geringer als die Pläne des Parlaments – höchstens 250.000 Euro oder 0,5% des Jahresumsatzes eines Unternehmens vorgesehen.[30]

7. Perspektiven

Seit dem 23.06.2015 versuchen im sog. *Trilog* die Kommission, das Parlament und der Rat, eine Einigung zu finden. Als zeitliches Ziel für eine politische Einigung wird Ende des Jahres 2015 angegeben. Ein Inkrafttreten der EU-DSGVO ist dann nach etwa zwei weiteren Jahren geplant. Der Trilog wird entscheidend sein für Umfang, Inhalt und Wirksamkeit des künftigen Datenschutzes in Europa. Es ist davon auszugehen, dass sich die Ergebnisse im Rahmen dessen halten werden, der von den drei EU-Gremien festgelegt wurde. Die Wirtschaftslobby wird versuchen, ihren Einfluss zur Geltung zu bringen. Die Datenschutzbeauftragten in Deutschland haben mit einem Text signalisiert, welche Schwerpunkte aus deren Sicht gesetzt werden müssen.[31] Es ist nicht auszuschließen, dass sich der EuGH mit einer Entscheidung zu Safe Harbor in die für die EU-DSGVO wichtige Frage nach Auslandsübermittlungen einmischen wird.[32] Bei den kommenden Diskussionen wird die öffentliche Debatte eine wichtige Rolle spielen. Insofern sind die Nichtregierungsorganisationen aufgefordert, ihre Positionen darzulegen und dafür zu sorgen, dass die Gespräche zwischen den Trilog-Verhandlungsparteien transparent geführt werden und dass dabei die öffentliche Meinung als ein wichtiger Beitrag mit berücksichtigt wird.

1 Nachweise bei Simitis in Simitis, BDSG, 8. Aufl. 2014, Einl. Rn. 178.

2 EGMR, Rotaru vs. Rumänien, U. v. 04.05.2000, Nr. 28341/95.

3 Siemen, Datenschutz als europäisches Grundrecht, 2006, S. 132 f.

4 BVerfGE 65, 43 = NJW 1983, 422.

5 BVerfG NJW 2010, 839, Rn. 218.

6 EuGH Rs. 29/69, Slg. 1969, 419 Rn. 7.

7 EuGH, C-293/12, C-594/12, NJW 2014, 2149.

8 Nachweise bei Simitis in Simitis, BDSG, 8. Aufl. 2014, Einl. Rn. 203.

9 2002/58/EG.

10 2009/136/EG

11 2006/24/EG.

12 EuGH NJW 2014, NVwZ 2014, 709 = DVBl 2014, 708.

13 EuGH, C-518/07, NJW 2010, 1265, C-614/10, ZD 2012, 563.

14 EuGH, C-28/08 P, K&R 2010, 574; vgl. Hustinx, in Schmidt/Weichert, Datenschutz, 2012, S. 322.

15 EuGH, C-468/10, DÖV 2012,201.

16 EuGH, C-131/12, AfP 2014, 245.

17 EuGH, C-212/13, NJW 2015, 463.

18 Empfehlung Nr. R(87)15 v. 17.09.1987.

19 Weichert RDV 2012, 113.

20 Weichert DuD 2014, 831.

21 KOM(2010) 609 endg. = BR-Drs. 707/10.

22 Vorschlag für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, COM (2012)0011-C7-0025/2012-2012/0011(COD); Spary DANA 1/2012, Gola/Schulz RDV 2013, 1; 4; Dehmel/Hullen ZD 2013, 147; Kipker/Voskamp DuD 2012, 737; Ronellenfitsch DuD 2012, 561; von Lewinski DuD 2012, 564; Jaspers DuD 2012, 571; Richter DuD 2012, 576; Schild/Tinnefeld DuD 2012, 312; Reding ZD 2012, 195; zum Arbeitnehmerdatenschutz Franzen DuD 2012, 322; Wybitul/Rauer, ZD 2012, 160; Gola/Schomerus, BDSG, 12. Aufl. 2015, Einl. Rn. 28 f.; DuD-Schwerpunktheft 10/2013 mit Beiträgen von Mester, Eckhardt, Kramer, Schießler, Zöll, Wieszorek, Seifert, Albrecht.

23 Nguyen DuD 2013, 662.

24 EP LIBE, 2012/0011(COD); Albrecht, Finger weg von unseren Daten, 2014, S.

25 Roßnagel/Kroschwald ZD 2014, 495, zu Relevanz für bDSB Bittner RDV 2014, 183.

26 Becker, Der Spiegel 11/2015, S. 42 f.

27 Zahlreiche Anträge verwässern Entwurf zur EU-Datenschutz-Grundverordnung, www.datenschutz-praxis.de 12.03.2015.

28 Dok. 9565/15.

29 Weichert DuD 2013, 246.

30 Krempl, www.heise.de 15.06.2015; Schulzki-Haddouti, c´t 2015, Heft 8 S. 40 f.

31 Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen zur Datenschutz-Grundverordnung, 2015.

32 ULD begrüßt Safe-Harbor-Vorlage wegen Facebook beim EuGH, https://www.datenschutzzentrum.de/artikel/213-.html.

Auf den nächsten Seiten finden Sie die Beiträge der folgenden Organisationen, Verbände und Einzelpersonen, die sich mit den roten Linien, welche bei den Trilog-Verhandlungen zur EU-DSGVO nicht überschritten werden dürfen, auseinandersetzen (in alphabetischer Reihenfolge): BfDI – Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, BvD – Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V., Digitalcourage – Digitalcourage e.V., Digitale Gesellschaft – Digitale Gesellschaft e. V., FIfF – Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V., GDD – Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V., Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Prof. Douwe Korff, Peter Schaar, vzbv – Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. (vzbv), Prof. Dr. Peter Wedde

BfDI – Andrea Voßhoff / Sven Hermerschmidt[1]

„Wo sind die roten Linien, die bei den Trilog-Verhandlungen in den kommenden Monaten nicht überschritten werden dürfen?“



Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit sieht die Einigung im Rat der Justiz- und Innenminister vom 15.6.2015 grundsätzlich positiv, denn damit ist die seit langem überfällige Reform des Europäischen Datenschutzrechts einen ganz entscheidenden Schritt vorangekommen. Auch aus inhaltlicher Sicht kann sich das Ergebnis vielfach durchaus sehen lassen. Gleichwohl gibt die Fassung des Rates in einigen Punkten Anlass zur Kritik.

Die rote Linie verläuft salopp gesagt entlang des geltenden Rechts und des derzeit vorhandenen Datenschutzniveaus. Sie wird mit anderen Worten dann überschritten, wenn die Datenschutz-Grundverordnung hinter das derzeitige Datenschutzniveau zurückfällt. Die sich aus Artikel 8 der Grundrechtecharta und Art. 16 Abs. 1 AEUV ergebenden Grundprinzipien des Datenschutzes dürfen daher nicht zur Disposition stehen. Gerade in Zeiten von Big Data und globaler Datenverarbeitung sind die Autonomie des Einzelnen, Transparenz und Rechtmäßigkeit der Datenverarbeitung, die Zweckbindung oder die Verantwortlichkeit des Datenverarbeiters ebenso wichtige Elemente der Grundrechtsgewährleistung wie eine starke Datenschutzaufsicht und wirksame Sanktionen.

Zur Illustration sollen zwei der wichtigsten Themen hier genannt werden:

1. Die Zweckbindung ist eines der zentralen Prinzipien des Datenschutzrechts. Sie dient der Transparenz und Vorhersehbarkeit der Verarbeitung personenbezogener Daten und stärkt damit die Autonomie des Einzelnen. Angesichts der Unsichtbarkeit und des Umfangs der Datenverarbeitung muss sich der Einzelne darauf verlassen können, dass seine personenbezogenen Daten grundsätzlich nur zu den Zwecken weiterverarbeitet werden, zu denen sie erhoben worden sind. Art. 8 Abs. 2 der Europäischen Grundrechtecharta hat daher die Zweckbindung als tragendes Prinzip des Datenschutzes verankert.
   Die Entwürfe der Kommission, aber vor allem des Rates, weichen die Zweckbindung in gefährlicher Weise auf. Zum einen sehen sie – im Unterschied zur geltenden Richtlinie 95/46/EG – vor, dass personenbezogene Daten auch zu solchen Zwecken weiterverarbeitet werden dürfen, die mit dem ursprünglichen Zweck nicht vereinbar sind. Der Rat will dies darüber hinaus zulassen, wenn der Datenverarbeiter ein überwiegendes berechtigtes Interesse an dieser Zweckänderung hat. Damit wird ohne Not die geltende Rechtslage verändert und das Prinzip der Zweckbindung sehr weit ausgehöhlt. Aus meiner Sicht muss es daher beim geltenden Prinzip bleiben, dem sich das Europäische Parlament in seinem Entwurf auch verschrieben hat.

2. Zentrale Legitimation für die Zulässigkeit der Verarbeitung personenbezogener Daten ist weiterhin die Einwilligung des Betroffenen. Recht auf informationelle Selbstbestimmung bedeutet, dass jeder selbst über Preisgabe und Verwendung seiner personenbezogenen Daten entscheiden kann. Die Einwilligung sichert diese Autonomie und ist daher auch in Art. 8 Abs. 2 der EU-Grundrechtecharta als Legitimation für die Verarbeitung personenbezogener Daten erwähnt.
   Diese zentrale Funktion der Einwilligung kann aber nur dann erfüllt werden, wenn sich der Einzelne der Tragweite und Bedeutung seiner Entscheidung bewusst wird. Dies erfordert eine ausdrückliche Willensbekundung des Betroffenen. Der Rat relativiert dies in seinem Vorschlag, in dem er eine unmissverständliche Einwilligung ausreichen lässt. Damit wird es insbesondere global agierenden IT-Unternehmen ermöglicht, durch die Verwendung pauschaler Datenschutzbestimmungen und datenschutzunfreundlicher Voreinstellungen weitreichende Datenverarbeitungsbefugnisse ohne eine ausdrückliche Einwilligung des Nutzers für sich zu reklamieren.
   Im Trilog sollte daher die Fassung von Kommission und Parlament zugrunde gelegt werden.

1 Die Autorin Voßhoff ist Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, der Autor Hermerschmidt ist dort Referent und Leiter der Projektgruppe „Revision des Europäischen Datenschutzrechts“.

BvD – Rudi Kramer / Thomas Spaeing

Wo sind die roten Linien?

Die Diskussion um die EU-Datenschutzgrundverordnung (EU-DSGVO) wird sehr kontrovers geführt. Wirtschaftliche Interessen und Bürgerrechte stehen sich vermeintlich unvereinbar gegenüber. Dabei verfolgt die Überarbeitung der europarechtlichen Datenschutzregelungen – ebenso wie die Richtlinie aus 1995 – zwei Ziele:

- den Schutz der natürlichen Person bei der Verarbeitung personenbezogener Daten
- und den freien Datenverkehr.

Zwangsläufig kollidieren diese beiden Ziele in Einzelfällen. Die roten Linien aus Sicht des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V. werden dann überschritten, wenn das Ziel des Schutzes der natürlichen Person bei der Verarbeitung personenbezogener Daten nicht erreicht wird.

Grundrechtsschutz beachten

Maßstab für den Schutz der natürlichen Person bei der Verarbeitung personenbezogener Daten für die Gestaltung der EU-DSGVO sind die Grundwerte des Art. 8 der Charta der Grundrechte der Europäischen Union.

Daraus ergibt sich als Konsequenz, dass personenbezogene Daten nur unter Beibehaltung des Grundsatzes Verbot mit Erlaubnisvorbehalt, also auf Basis einer Rechtsgrundlage verarbeitet werden dürfen. Dies schließt auch die Möglichkeit der Einwilligung durch die betroffene Person ein. Die in der Charta ausdrücklich genannte Überwachungsinstanz der unabhängigen Stelle wird europaweit durch die Aufsichtsbehörden und darüber hinaus in Deutschland heute erfolgreich durch die innerbetriebliche Selbstkontrolle durch die Funktion des Datenschutzbeauftragten wahrgenommen.

Zweckbindung ist Grundrechtsmerkmal

Ein weiteres mit Grundrechtschutz versehendes Merkmal ist die Zweckbindung der Verarbeitung personenbezogener Daten in der Grundrechtscharta. Zweckänderungen nach Treu und Glauben für verwandte Zwecke lassen sich unter bestimmten gesetzlichen Voraussetzungen wie der Vorhersehbarkeit gegebenenfalls rechtfertigen. Aber eine eigenmächtige Zweckänderung des Datenverarbeiters für mit dem eigentlichen Zweck nicht-kompatible Ziele ist unter Beibehaltung eines Personenbezugs mit der Grundrechtscharta kaum vorstellbar. Selbstverständlich werden betroffene Personen aber auch nicht gehindert, einer Zweckänderung zustimmen zu dürfen. Eine wesentliche Zweckänderung der Verarbeitung personenbezogener Daten ohne Einbeziehung der betroffenen Person wäre daher eine solche rote Linie.

Die Merkmale des Transparenzgebotes im Datenschutz wie Auskunftsrecht und ein Berichtigungsanspruch sind weitere Leitplanken, die der europäische Gesetzgeber bei der EU-DSGVO zu beachten hat. Ein Anspruch auf Datenportabilität aber, auch wenn er in Einzelfällen bei dem Wechsel einzelner Dienstleistungen auf den ersten Blick nützlich erscheinen mag, bringt jedoch weitere offene Probleme mit sich: Was nützt eine Datenportierung bei einem Online-Bestellsystem? Auch bei einem sozialen Netzwerk stellt sich die Frage, wie sichergestellt werden soll, dass alle bisherigen Kontaktpersonen aus Netzwerk „A" damit einverstanden sind, mit der gemeinsamen Kommunikation nun auch unter Geltung der Allgemeinen Geschäftsbedingungen des Netzwerks „B" eingestellt zu werden? Hier werden mehr Fragen aufgeworfen, als durch die Neuregelung im Entwurf der EU-Kommission gelöst.

Wirksame Aufsichtsstrukturen

Allein aus dem Schutzbereich des Art. 8 der Charta der Grundrechte lässt sich auch die Überwachung durch eine unabhängige Aufsicht herleiten. Hierdurch werden die natürlichen Personen innerhalb der Europäischen Gemeinschaft auch vor Zugriffsmöglichkeiten und Begehrlichkeiten der einzelnen Mitgliedsstaaten geschützt. Dieser Schutzbereich ist aufgrund der Grundrechtsformulierung unabhängig von einer Bürgereigenschaft zu einem Mitgliedsstaat der Europäischen Union. Damit werden auch betroffene Personen umfasst, die keine Bürger der Europäischen Union sind, deren Daten dort aber verarbeitet werden. Die Ausgestaltung dieser Schutzbehörde muss auch einen angemessenen Schutz gewährleisten, um diese Grundrechtsregelung nicht auszuhöhlen.

In Deutschland hat sich mit den 2-Säulen eines staatlichen und betrieblichen / behördlichen Datenschutzbeauftragten ein System bewährt, dass im Rahmen einer regulierten betrieblichen Selbstkontrolle den Verarbeitungsverantwortlichen und Auftragsverarbeitern die Möglichkeit gibt, Aufgaben der Beratung, der Dokumentation und Kontrolle intern zu übernehmen. Zeitaufwändige Abstimmung mit staatlichen Aufsichtsbehörden werden dadurch auf ein Minimum reduziert, kompetente Ansprechpartner mit spezialisiertem Branchen-Know-How können frühzeitig in die Planung komplexer Projekte einbezogen werden und ein Scheitern aufgrund von zu spät erkannten Datenschutzverstößen verhindern. Um dieser Aufgabe gerecht zu werden, ist es zwangsläufig erforderlich, dass der betriebliche / behördliche Datenschutzbeauftragte seine Aufgabe ohne Furcht vor Repressalien ausüben kann, Anspruch auf adäquate Aus- und Fortbildung hat, einer Verschwiegenheitspflicht unterworfen und durch ein Benachteiligungsverbot geschützt wird. Aus Sicht der Unternehmen – aber auch der staatlichen Aufsichtsbehörden – ist es zudem erforderlich, dass der betriebliche / behördliche Datenschutzbeauftragte auch Aufgaben übernehmen kann und muss, die sonst über zentralistisch

organsierte Aufsichtsbehörden bearbeitet werden müssten wie bei Regelungen zur vorherigen Zurateziehung. Hier sind aus Sicht der verarbeitenden Wirtschaft zeitliche Verbesserungen bei der Bearbeitung erforderlicher datenschutzrechtlicher Klärungen zu erreichen. So kann der betriebliche / behördliche Datenschutzbeauftragte die Aufsichtsbehörden bei der vorherigen Zurateziehung nach Art. 34 EU-DSGVO entlasten, sowie bei Kontroll- und Beratungsaufgaben. Die besondere Stärke dieses Modells wird deutlich in dem erforderlichen Schutz der natürlichen Personen sowie in der schnellen und praxisnahen Bearbeitung der datenschutzrelevanten Vorgänge in den Unternehmen vor Ort und damit in der schneller erreichten Rechtssicherheit für die Beteiligten.

Datenverarbeitung ermöglichen

Letztendlich definieren sich für den BvD die roten Linien der EU-DSGVO aber auch danach, wie das zweite Ziel, der freie Datenverkehr erreicht wird. Die Verarbeitung personenbezogener Daten muss unter Berücksichtigung der Interessen der betroffenen Person möglich sein. Kaum ein Wirtschaftszweig ist ohne Datenverarbeitung vorstellbar. Und bei den meisten Unternehmungen erfolgt die Datenverarbeitung nur als Nebenschauplatz der unternehmerischen Tätigkeit, wenn es um die Verarbeitung der Beschäftigten- oder Kundendaten geht. Zu umfassende Einwilligungsvoraussetzungen können dem entgegenstehen, wenn dadurch auch keine weitere Rechtssicherheit für die betroffene Person gewährleistet wird. Auch müssen Informationspflichten so gestaltet sein, dass sie durch die betroffene Person noch wahrgenommen werden können und sich auf die wesentlichen Aussagen beschränken, um die Zielgruppe nicht durch seitenlange „ausufernde“ Informationen zu überfordern. Welchen Stellenwert hat beispielsweise die Angabe über die voraussichtliche Speicherdauer gegenüber der betroffenen Person bei der Datenerhebung, wenn die wesentlichen Informationen handels- oder steuerrechtlichen Aufbewahrungsvorschriften unterliegen? Die Rechtmäßigkeitsvoraussetzungen für die Verarbeitung personenbezogener Daten müssen auch für kleine und mittlere Unternehmen (KMU) klar und verständlich anwendbar sein – auch ohne Einbeziehung eines spezialisierten Rechtsanwalts. Dabei sind auch Erleichterungen für KMUs zu hinterfragen: Diese dürfen nicht dazu führen, dass das Ziel des Schutzes der natürlichen Person eingeschränkt wird, nur um KMUs die Verarbeitung zu ermöglichen. Das bisherige Schutzkonzept aus Eigenverantwortlichkeit des Unternehmens, staatlicher Aufsicht und interner Beratung und Überwachung durch einen durch das Unternehmen selbst ausgewählten (auch externen) Datenschutzbeauftragten bietet auch hier die Gewähr für eine angemessene Interessensberücksichtigung. Einen Grundrechtsschutz durch die Unternehmensgröße in Form der Mitarbeiterzahl zu begrenzen wäre ungewöhnlich und europarechtlich fraglich. Denn gerade in diesem Bereich benötigen die Unternehmen aller Größenordnungen Rechtssicherheit durch die Funktion des Datenschutzbeauftragten.

So wird die Wirksamkeit der geforderten Schutzmaßnahmen ohne betriebliche / behördliche Datenschutzbeauftragte allein von der Ausstattung und der Kontrollfähigkeit starker Aufsichtsbehörden abhängen, ein Ansatz, der an das 19. Jahrhundert erinnert und jegliche positive Erfahrungen zur regulierten Selbstkontrolle der letzten 20 Jahre unter der RL EU 95/46 EG außen vor lässt.

Und wie definiert man letztendlich die „roten Linien“, wenn sich herausstellt, dass die personelle Ausstattung der Aufsichtsbehörden einen Flaschenhals darstellt, der sich negativ auf die beiden Ziele der EU-DSGVO auswirkt? Wenn weder aufgrund unzureichender Kontrollen der Schutz der natürlichen Person vor unrechtmäßiger Verwendung der Daten sichergestellt werden kann, noch der rechtssichere, freie Datenverkehr gewährleistet ist, weil die Anfrage über Art. 34 bei der Zurateziehung der Aufsichtsbehörden zu Verzögerungen bei der Einführung von Geschäftsmodellen oder Verarbeitungstechniken führt? Zumal die Aufsichtsbehörden ihr Personal auf die Fälle priorisieren werden, bei denen wie im Kohärenzverfahren enge zeitliche Reaktionszeiten vorgegeben sind.

Der Berufsverband der Datenschutzbeauftragten (BvD) e.V. sieht unüberschreitbare rote Linien für den europäischen Gesetzgeber bei der Gestaltung der EU-DSGVO stets in der Verletzung des Grundrechtsschutzes der natürlichen Person oder aber in großem Formalismus, ohne dass aus ihm ein Mehrwert für die natürliche Person oder für das Unternehmen ein Mehrwert unter Berücksichtigung der Interessen der natürlichen Person erlangt wird. Die Funktion des betrieblichen / behördlichen Datenschutzbeauftragten ist darauf ausgerichtet, auf die Einhaltung genau dieser Grenzen tagaktuell hinzuwirken – eine Aufgabe, die durch behördliche Kontrolle keinesfalls in gleicher Effizienz und Wirtschaftlichkeit erfüllt werden kann.

Ihr BvD-Ansprechpartner:

Vorstandsvorsitzender Thomas Spaeing, Budapester Straße 31, 10787 Berlin, Tel: 030 . 26 36 77 60,
E-Mail: bvd-gs@bvdnet.de,
Internet: https://www.bvdnet.de

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. fördert die beruflichen Interessen seiner Mitglieder, der Datenschutzbeauftragten in Behörden und Betrieben. Er setzt sich aktiv für die Etablierung des Berufsbildes „Datenschutzbeauftragter“ in Deutschland ein. Dazu bündelt er Fragen aus der Praxis und arbeitet kontinuierlich an der Definition des Berufsbildes.

Der BvD bietet das kompetente Netzwerk für die tägliche Berufsausübung und stellt einen permanenten Austausch mit Vertretern aus Wirtschaft, Wissenschaft, Politik und Aufsichtsbehörden sicher. Dazu gehört die Mitarbeit bei wichtigen Gesetzgebungsverfahren. Dies geschieht bspw. durch öffentliche Stellungnahmen und in Hintergrundgesprächen mit Politikern, Aufsichtsbehörden und Journalisten. Zusätzlich informiert er regelmäßig Entscheider aus Wirtschaft und Politik über das Berufsbild sowie über die Leistungen des Datenschutzbeauftragten und betreibt gezielte Öffentlichkeitsarbeit.

Digitalcourage

Fünf rote Linien für Datenschutz in Europa

Die Europäische Union hat vor mehr als drei Jahren eine Datenschutzreform begonnen, die neue Verordnung darf auf keinen Fall hinter die bestehenden Regeln aus dem Jahr 1995 zurückfallen.

Jetzt sind die Verhandlungen im Trilog entscheidend für die Zukunft des Datenschutzes in Europa und damit für zahlreiche Grundrechte im digitalen Zeitalter.

Fünf rote Linien müssen in den Trilog-Verhandlungen unbedingt eingehalten werden:

Mit der Datenschutzreform muss der EU der große Wurf gelingen. Datenschutz muss zeitgemäß werden – das heißt, ein Zurückfallen hinter die alte Richtlinie darf es nicht geben!

Jetzt ist der Trilog entscheidend für die Zukunft des Datenschutzes in Europa und für unsere Grundrechte im digitalen Zeitalter.

Wir zeigen fünf Grenzen, die nicht überschritten werden dürfen:

1 Prinzipien der Speicherung

In Artikel 5 hat der Ministerrat das Prinzip der Datensparsamkeit zurückgefahren: Statt „limited to the minimum necessary" – also aufs notwendigste beschränkt – sollen Datensammlungen jetzt „not excessive" sein. Das ist ein klarer Rückschritt. Datensparsamkeit muss ein starkes Prinzip bleiben. Nur Datensammlung, die sich auf das Notwendigste beschränken, sind akzeptabel.

Artikel 23 beinhaltet das von der Kommission neu eingebrachte Prinzip Datenschutz by design und by default. Datenverarbeiter sollen so wenig Daten wie möglich verarbeiten und nicht benötigte Daten so schnell wie möglich löschen. Dieses Prinzip stärkt den Datenschutz, weil es Datensammlungen auf Vorrat unmöglich macht.

Der Artikel muss unbedingt folgende Punkte enthalten: „state of the art technology", „international best practices", „technical measures" und „orginisational measures". Die vom Rat vorgeschlagene „Pseudonymisierung" muss explizit aus dem Artikel gestrichen werden, weil sie nichts daran ändert, dass private Daten erhoben und verarbeitet werden.

2 Zweckbindung ohne Ausnahmen

Die Zweckbindung ist essentiell für die nachvollziehbare Verarbeitung von Daten. Nur mit einer starken Zweckbindung werden Verbraucher.innen zukünftig geschützt vor: versteckten Datenbanken, ungewolltem Scoring, Datenhandel oder weiteren, heute nicht abschätzbaren Eingriffen in Grundrechte. Artikel 6.4. muss ersatzlos gestrichen werden. Auch Artikel 6, Absatz 3a muss ersatzlos gestrichen werden, weil er unzweckmäßige Datenverarbeitung erlaubt.

3 Profilbildung nur mit expliziter Zustimmung

Das in Artikel 19 geregelte Profiling sollte nur durch explizite Zustimmung erlaubt werden, weil mit diesen Verfahren nicht abschätzbare Gefahren für die Privatsphäre von Menschen einhergehen.

Rat und Kommission bieten nur an, dass den Ergebnissen eines Profilings widersprochen werden kann, beziehungsweise, dass nur widersprochen werden kann, wenn erhebliche Auswirkungen vorliegen.

Diese Einschränkungen sind inakzeptabel, da jedes Profiling, wie etwa Kauf-, Bewegungs- oder Kommunikationsprofile genau den Zweck hat, Auswirkungen auf das Verhalten von Menschen auszuüben. Die Position des Parlaments („the data subject shall be informed about the right to object to profiling in a highly visible manner.") muss ergänzt werden: Wer gegen Profiling widerspricht, darf nicht diskriminiert werden, etwa, indem der Abschluss eines Vertrags oder die Nutzung eines Dienstes verwehrt wird.

4 Auskunftsrechte immer kostenfrei!

Artikel 15 regelt Auskunftsrechte und ist damit die Basis für das Grundrecht auf informationelle Selbstbestimmung. Wer seine Auskunftsrechte wahrnehmen will, darf auf keinen Fall durch Gebühren davon abgehalten werden. Die Version des Rates sieht aber genau das vor und schwächt die Auskunftsrechte noch weiter: Unter Berufung auf Urheberrechte oder Geschäftsgeheimnisse sollen Auskünfte an Verbraucher.innen verweigert werden können. Damit könnten Anfragen pauschal abgelehnt werden.

Auskunftsrechte müssen kostenlos sein, den vollen Umfang der Daten und Datenkategorien umfassen, den Zweck und die Dauer der Speicherung sowie die Herkunft der Daten beinhalten und darüber informieren, welche Daten an wen – auch international oder im Rahmen von firmeninternen Austauschen – weitergegeben wurden.

Es muss darauf hingewiesen werden, an welche Aufsichtsbehörde Beschwerden gerichtet werden können und eine Kopie der Daten muss – falls gewünscht – kostenlos im maschinenlesbaren Format bereit gestellt werden, sofern die Daten in einem solchen gespeichert sind.

5 Datenportabilität ermöglichen

Artikel 18 regelt die Portabilität von Daten und gibt Verbraucher.innen damit die Möglichkeit Dienste wechseln zu können. Das ist Voraussetzung für Wettbewerb zwischen Dienst-Anbietern und für Nutzer.innen unumgänglich, weil es möglich sein muss, zum Beispiel Daten aus einem sozialen Netzwerk in ein anderes problemlos „umziehen" zu können. Deshalb braucht es Datenportabilität in einem „electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn."

Digitale Gesellschaft – Alexander Sander

Der Datengier gewidmet

Seit 2012 streitet man auf europäischer Ebene über die Datenschutzreform, um die bestehende Regulierung aus dem Jahr 1995 endlich fit für die digitale Gesellschaft zu machen. Doch was als ambitioniertes Projekt begann, droht in einem Desaster für Verbraucherinnen und Verbraucher zu enden. Unternehmen, die mit unseren Daten Millionen scheffeln, torpedieren seit Jahren durch intensive Lobbybemühungen den Gesetzgebungsprozess – offensichtlich mit Erfolg. Denn nun setzen sich die Mitgliedsstaaten der EU dafür ein, den vom EU-Parlament erzielten Kompromiss für mehr Datenschutz bis zur Unkenntlichkeit aufzuweichen.

Täglich produzieren wir Unmengen von Daten, die viel über unser Privatleben aussagen – welche Seiten wir im Internet besuchen, wo wir uns gerade befinden oder mit wem wir kommunizieren. Oft sind jedoch nur sehr wenige dieser Informationen vonnöten, damit Unternehmen einen bestimmten Dienst anbieten können. Die Datengier von Unternehmen aber ist prinzipiell unbegrenzt, denn mit jeder zusätzlichen Information lässt sich zusätzliches Geld verdienen. Immer mehr Daten werden gespeichert und ausgewertet, ohne dass Verbraucherinnen und Verbraucher dies wissen und wollen. Dieser Praxis sollte durch die Reform ein Ende bereitet werden. Daten sollten nur zu ganz bestimmten, vorher festgelegten Zwecken erhoben und verarbeitet werden dürfen. An diesem Prinzip der „Zweckbindung" der Daten – etwa dass eine Adresse nur zum Versand eines Produktes genutzt werden darf, nicht aber für Werbung – wird nun gerüttelt.

Nach Ansicht des Rates der Europäischen Union soll die Zweckbindung wegfallen, wenn die Unternehmen oder sogar Drittanbieter ein „berechtigtes Interesse" an der Verarbeitung der Daten haben und dieses gewichtiger ist als die Interessen der Verbraucherinnen und Verbraucher. Geht die Abwägung zugunsten der Unternehmensinteressen aus, spielt die Zweckbindung keine Rolle mehr. Obendrein sind es stets die Datenverarbeiter selbst, die diese Abwägung vornehmen. Faktisch wie juristisch fallen damit die Hürden für eine uferlose Verwendung der Kundendaten. Ohne dass es der Zustimmung von Verbraucherinnen und Verbrauchern oder einer Zweckbestimmung bedarf, können Unternehmen die Daten nach Belieben verarbeiten und weitergeben. Somit gehen die Informationen auch an Firmen, welche die Betroffenen weder kennen, noch deren Datenverarbeitungen sie zugestimmt haben.

Sollte die Regulierung in dieser Form verabschiedet werden, können wir künftig kaum mehr nachvollziehen, wer unsere Daten zu welchen Zwecken verarbeitet. Damit löst sich ein Grundkonzept der Datenschutzreform in Luft auf. Der Rat leistet so einem klaren Verstoß gegen das Grundrecht auf informationelle Selbstbestimmung und die europäische Grundrechtecharta Vorschub.

Doch nicht nur die Zweckbindung steht auf der Kippe, auch das Zustimmungsprinzip soll geschwächt werden: Während man sich im EU-Parlament auf eine „explizite" Zustimmung für die Datenverarbeitung verständigt hat, will der Rat diese aufweichen und durch eine „eindeutige" Zustimmung ersetzen. Mit dieser schwammigen Definition wird dem Missbrauch Tür und Tor geöffnet.

Ähnlich verwässern will der Rat auch das Prinzip der Datensparsamkeit. Statt, wie das EU-Parlament vorgesehen hat, Daten nicht über das notwendige Mindestmaß hinaus anzuhäufen, schreibt der Rat vor, dass Daten „nicht exzessiv" gesammelt werden sollen.

Den Unternehmen wird es so ermöglicht, Daten zu beliebigen Zwecken zu erheben, zu verarbeiten und an Dritte weiterzugeben. Statt robuste Datenschutzregeln festzulegen, die Verbraucherinnen und Verbraucher ermächtigen, selbstbestimmt die Kontrolle über ihre Daten zu erhalten, soll die schier unermessliche Gier datenhungriger Unternehmen bedingungslos befriedigt werden. Statt ein europäisches Modell für den Datenschutz zu etablieren, wird dem US-amerikanischen Datenmonster-Vorbild nachgeeifert.

Damit die Reform doch noch einen echten Datenschutz garantiert, muss das EU-Parlament in den den Trilog-Verhandlungen die eigenen Position verteidigen und vor allem dem Rat die Grenzen aufzeigen. Das EU-Parlament muss sich gegen die Lobbyinteressen der Datenkraken stellen, die derzeitig von den Mitgliedstaaten der EU vertreten werden, und für eine Datenschutzreform kämpfen, die ihren Namen verdient.

FIfF e.V.

Rote Linien

Nachdem die Datenschutzstandards in der Praxis des globalen Datenverkehrs immer mehr aufgeweicht wurden, schafft die Datenschutzgrundverordnung die Möglichkeit, bei einem europäischen Grundrecht in die Offensive zu gehen. Das FIfF hat sich in den Diskussionsprozess mehrfach eingebracht und Vorschläge für eine datenschutzfreundlichere Zukunft gemacht. Die letzten Entwicklungen um den Entwurf des Ministerrates zeigen aber deutlich, dass der Wirtschaftslobbyismus funktioniert und nicht alle Interesse an einem starken europäischen Datenschutz haben. Es ist beschämend, dass gerade Deutschland mit allein 51 Forderungen den Parlamentsvorschlag beschädigt hat. Die gemeinsame Position des Rats der Europäischen Union vom 15. Juni 2015, 9565/15, überschreitet diverse rote Linien und fällt hinter die Standards der Datenschutz-Richtlinie von 1995 zurück.

Einwilligung

Bisher tun die Anbieter von Dienstleistungen im Internet häufig so, als bedeute schon die Nutzung eines Dienstes oder das Nichthandeln eine stillschweigende Einwilligung. In Artikel 7 wollen Parlament und Kommission sicherstellen, dass der betroffenen Person im Sinne einer informierten Einwilligung bewusst ist, dass sie ihre Einwilligung gibt. Eine ausdrückliche Handlung möchte der Rat vermeiden und fügt im Erwägungsgrund 25 ein, dass die Einwilligung auf „*beliebige*“ geeignete Weise und nur „*eindeutig*“ statt „*ausdrücklich*“ erfolgen soll. Schon die Einstellungen des Browsers oder einer anderen Anwendung sollen eine Einwilligung signalisieren können.

Will eine Person eine Einwilligung widerrufen, soll das nach dem Wunsch des Europäischen Parlaments so einfach sein wie das Erteilen der Einwilligung, als die ja schon der Besuch einer Website gesehen werden kann. Diese Forderung im Artikel 7 hat der Rat gestrichen.

Bei diesem Grundpfeiler des Datenschutzes ist so viel Entgegenkommen gegenüber den Datenkraken mit uns nicht zu haben!

Datensparsamkeit

In Artikel 5 Satz 1 (c) haben Parlament und Kommission in wünschenswerter Klarheit festgelegt, dass die zu erhebenden personenbezogenen Daten auf das für die Zwecke „*notwendige*“ Maß beschränkt sein müssen. Der Rat weicht den Zweckbezug zu „*verhältnismäßig*“ auf. An anderer Stelle (Erwägungsgrund 39) will der Rat die Verhältnismäßigkeit den Betreibern von elektronischen Kommunikationsnetzen und -diensten sowie Anbietern von Sicherheitstechnologien und -diensten erlassen. Dagegen verlangt das Europäische Parlament, dass die Verarbeitung „*für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig*“ sein muss.

An vielen Stellen hat der Rat die Vorgaben zur Datensparsamkeit gestrichen, die das Parlament eingeführt hat. In Erwägungsgründen 61 und 125 „*kann*“ sie eine Maßnahme sein, in Artikel 23 wird sie lediglich als ein Beispiel genannt, die Rechte der Betroffenen zu schützen. Lobby-Arbeit hat wohl auch dazu geführt, dass laut Erwägungsgrund 30 personenbezogene Daten verarbeitet werden dürfen, wenn sich der Zweck anders nicht „*in zumutbarer Weise*“ erreichen lässt. Schwammiger lässt sich die Datensparsamkeit kaum dem Ermessen der Unternehmen anheim stellen.

Bei der Verarbeitung personenbezogener Daten zu historischen, statistischen oder wissenschaftlichen Forschungszwecken (Erwägungsgrund 125) wünscht sich der Rat weitere Register mit den Daten großer Bevölkerungsanteile (auch Verstorbener, Erwägungsgrund 23). Das sind Sammlungen, die wachsende Begehrlichkeiten auf sich ziehen werden.

Datensparsamkeit als Anforderung endlich durchsetzbar zu machen, das wollen die Minister nicht. Wir bestehen auf den Formulierungen des Parlaments!

Zweckbindung

Der Entwurf des EU-Rats will es ins Ermessen der Unternehmen legen, den Zweck einer Verarbeitung nach Belieben neu zu definieren. Statt dass Daten gelöscht werden, wenn sie ihren Zweck erfüllt haben, will der Rat in Erwägungsgrund 40 und Artikel 6 Satz 3a (a) eine Zweckänderung erlauben, wenn der neue Zweck mit dem ursprünglichen Zweck „*vereinbar*“ ist.

Im Erwägungsgrund 39 haben die Minister zudem die „*Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung*“ als berechtigtes Interesse definiert – Wenn die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen, soll das zwar ausgeschlossen sein, informationelle Selbstbestimmung sieht aber anders aus. Betroffene können nicht sicher wissen, ob bei der Verarbeitung „*für nicht konforme Zwecke aufgrund der berechtigten Interessen dieses [...] Verantwortlichen oder eines Dritten*“ dessen Interessen überwiegen, was die Verarbeitung rechtmäßig macht (Artikel 6 Satz 4).

Bei diesem Grundpfeiler des Datenschutzes ist so viel Entgegenkommen gegenüber den Datenkraken mit uns nicht zu haben!

Profile

Als Profiling sieht der Rat erst die Nutzung personenbezogener Daten an, die verarbeitet wurden, damit eine Person bewertet oder ihr Verhalten analysiert oder vorhergesagt werden kann (Artikel 4 (12a)). Das Parlament defi-

niert Profiling bereits über den Zweck, wodurch die Rechte der Betroffenen, beispielsweise Auskunfts- und Widerspruchsrecht, besser und früher greifen können, nicht erst dann, wenn womöglich eine Entscheidung gefallen ist. Der Rat hat das Profiling sogar aus dem Titel von Abschnitt IV und Artikel 20 gestrichen, um die automatisierte Entscheidungsfindung zum Ansatzpunkt für die Rechte der Betroffenen zu machen, nicht etwa schon das Profiling selbst. Es müssen rechtliche Folgen oder eine erhebliche Beeinträchtigung der Betroffenen vorliegen, bevor ihnen Möglichkeiten zum Widerspruch gegeben werden. Wo die Kommission noch von „*auf Profiling basierenden Maßnahmen*" spricht und das Parlament vom Profiling selbst, macht der Rat die Entscheidungsfindung zur Überschrift und das Profiling zur Nebensache.

Automatisierte Entscheidungsfindung und Profiling sogar auf der Grundlage besonderer Kategorien von personenbezogenen Daten sollen erlaubt sein, wenn eine Datenschutz-Folgenabschätzung stattgefunden hat (Erwägungsgrund 58), hier wird Diskriminierung zur Abwägungsfrage.

Wir im FIfF e.V. hatten eine Verschärfung der Profiling-Bestimmungen gefordert, der Rat schwächt sie noch weiter ab. So viel Entgegenkommen gegenüber den Datenkraken ist mit uns nicht zu haben!

Datenschutz durch Technik und Datenschutz-freundliche Voreinstellungen

Diese Prinzipien hatte die Kommission eingeführt und das Parlament zur Freude von Datenschützern zur Pflicht gemacht, der Rat hat sie abgeschwächt. Er will die Hersteller der Produkte, Dienste und Anwendungen lediglich „*ermutigen*", Datenschutz bei der Entwicklung der Produkte, Dienste und Anwendungen zu berücksichtigen. Neben den Verantwortlichen für die Datenverarbeitung will das Parlament die Hersteller für solche datenschutzfreundlichen Produkte verantwortlich machen (Erwägungsgrund 61). Der Rat hat diese Vorgabe des Parlaments aufgeweicht. Das Parlament weist in Artikel 23 ausdrücklich darauf hin, dass sich Datenschutz durch Technik in der Technikfolgen-Abschätzung auf das gesamte Lebenszyklus-Management der Verarbeitung bezieht. Diesen Hinweis hat der Rat ebenso gestrichen wie in Artikel 33 die Forderung des Parlaments zu dokumentieren, welche Maßnahmen getroffen wurden (Satz 3 g).

Wir haben die Neuerungen durch Parlament und Kommission begrüßt und hätten sie uns stärker gewünscht. Eine Abschwächung als Entgegenkommen gegenüber den Datenkraken ist mit uns nicht zu haben!

Unabhängige Kontrollen und Sanktionen

Entgegen dem Parlamentsbeschluss (Artikel 32a und 35) sieht der Rat keine *Pflicht* zur Einführung von Datenschutzbeauftragten vor, sie soll nur bestehen, wenn das nationale Recht dies vorsieht. Andernfalls „*kann*" oder „*darf*" der Verantwortliche einen Datenschutzbeauftragten benennen. Es muss nicht mehr sichergestellt sein, dass bei einer Gruppe von Unternehmen der Datenschutzbeauftragte von jedem Standort leicht zugänglich ist. Auch zur Vertraulichkeit über die Identität der betroffenen Person sollen Datenschutzbeauftragte nicht mehr verpflichtet sein (Artikel 36 Satz 4). Die vom Parlament geforderte Bereitstellung aller benötigten Mittel, darunter Personal, will der Rat nicht. In Artikel 35 Satz 10 wurde der Rechtsanspruch der Betroffenen, den Datenschutzbeauftragten zu Rate zu ziehen, abgeschwächt zu: „*Betroffene Personen* können *den Datenschutzbeauftragten [...] zu Rate ziehen*."

Im Artikel 79 haben sich nationale Interessen besonders deutlich niedergeschlagen, im vorauseilenden Gehorsam gegenüber den IT-Konzernen. Wo das Parlament Klartext redet und eine unabhängige Aufsichtsbehörde ermächtigt, Geldbußen bis zu 5% (im EP-Beschluss) ihres (Konzern-)Umsatzes oder einer Milliarde Euro zu verhängen, da erteilt der Rat den *Mitgliedstaaten* die Befugnis Gerichtsverfahren anzustrengen. Geldbußen dürfen die Aufsichtsbehörden selbst nur verhängen, wenn dies im nationalen Recht vorgesehen ist (Erwägungsgründe 100, 118b, 120, 120a und viele andere). Die Aufsichtsbehörde schrumpft zur rein nationalen Angelegenheit und ein Staat „*kann*" (Artikel 79 Satz 3b und 5) entscheiden, ob überhaupt Geldbußen verhängt werden sollen. Wenn ja, kann die Aufsichtsbehörde nur noch maximal 2 % des Umsatzes festlegen. Die Mitgliedstaaten setzen damit einen der größten Vorteile einer europaweiten und durchsetzbaren Verordnung außer Kraft. Wir müssen davon ausgehen, dass sich große Konzerne nun weiterhin ihren Hauptsitz danach auswählen werden, wo die geringsten Kontrollen und Sanktionen zu befürchten sind.

Statt einheitliche Kontroll- und Sanktionsstandards zu schaffen, wollen die Minister nationale Standortvorteile behalten. Diese Egoismen zu Lasten des Datenschutzes sind mit uns nicht zu haben!

Drittstaaten-Regelung

Weil Datenschutz in Europa ein verbindliches Grundrecht mit Verfassungsrang in der EU-Grundrechtecharta ist, dürfen personenbezogene Daten grundsätzlich nur innerhalb Europas verarbeitet werden. Das scheint nicht zu den Interessen von Konzernen zu passen, die immer mehr Daten benötigen für ihre Geschäfte mit Big Data oder Scoring. Es ist ganz im Sinne der IT-Monopolisten, als „*Big Data*" alles zu speichern, was irgendwie verarbeitet werden kann. Regelungen aus der Parlamentsvorlage für die Übertragung von Daten in Drittstaaten (Nicht-EU-Staaten) hat der EU-Rat durchlöchert. Zu Recht sieht er vermutlich die Freihandelsabkommen TTIP und TiSA dadurch gefährdet. Insbesondere die regulatorische Zusammenarbeit wird fatale Folgen für die informationelle Selbstbestimmung und den Grundrechtsschutz in der EU haben.

Eine Aufweichung der Drittstaaten-Regelung als Entgegenkommen gegenüber den Datenkraken ist mit uns nicht zu haben!

GDD

Keine EU-Datenschutz-Grundverordnung ohne den Datenschutzbeauftragten

1. Einleitung

Das Treffen der Justiz- und Innenminister im Juni diesen Jahres bestätigte das, was sich in den Verhandlungen im Rat der Europäischen Union über die letzten drei Jahre hinsichtlich einer EU-Datenschutz-Grundverordnung (EU-DS-GVO) bereits angedeutet hatte: Verantwortliche Stellen und Auftragsverarbeiter sollen nicht dazu verpflichtet werden, einen Datenschutzbeauftragten zu bestellen. Verwundern mag dieser zu Kommission[1] und Europäischem Parlament[2] konträre Standpunkt auf den ersten Blick nicht. Denn neben Deutschland sehen nur wenige Mitgliedstaaten[3] in ihren nationalen Gesetzen bis dato die vorgeschriebene Bestellung eines Datenschutzbeauftragten für nicht-öffentliche Stellen vor.

2. Bestellpflicht des Datenschutzbeauftragten

Nach Art. 35 Abs. 1 des Ratsentwurfs kann – bzw. sofern im Unionsrecht oder im nationalen Recht vorgesehen, muss – der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter einen Datenschutzbeauftragten benennen. Diese Öffnungsklausel soll es Mitgliedstaaten ermöglichen, über eigene nationalstaatliche Regelungen am Institut des Datenschutzbeauftragten festzuhalten. Diese Vorgehensweise läuft einerseits einem Harmonisierungsgedanken zuwider, andererseits bringt er auch negative Auswirkungen gerade für datenverarbeitende Stellen mit sich. Bei einem Verzicht auf den Datenschutzbeauftragten würde nicht nur eine unabhängige interne Compliance-Instanz zum Datenschutz fehlen, sondern auch eine Person, die im Hinblick auf die personenbezogene Datenverarbeitung als Anwalt der Betroffenen agiert. Ferner ist zu befürchten, dass Unternehmen wie Behörden in Ermangelung einer internen Compliance-Instanz zum Thema „Datenschutz" nur unzureichend die datenschutzrechtlichen Anforderungen bei der Verarbeitung von Daten Betroffener beachten. Darüber hinaus ist der Wegfall des Datenschutzbeauftragten auch unter Wirtschaftlichkeitsgesichtspunkten wenig sinnvoll. So müssten sich zur Befolgung der geplanten EU-Verordnung die Fachabteilungen in Behörden und Unternehmen die notwendigen datenschutzrechtlichen Kenntnisse selber aneignen, die bisher beim Datenschutzbeauftragten gebündelt waren, mit der Folge, dass erhebliche Synergieeffekte verloren gingen. Insofern ist der betriebliche Datenschutzbeauftragte ein wesentliches Element zur Entbürokratisierung der Datenschutzorganisation und -kontrolle.

Sollte sich der Ratsentwurf mit einer nationalen Öffnungsklausel trotz der aufgezeigten negativen Auswirkungen durchsetzen, weist die GDD darauf hin, dass eine Abkehr von einer obligatorischen Bestellung des behördlichen und betrieblichen Datenschutzbeauftragten nicht ohne die Schaffung von gesetzlichen Anreizen für dessen freiwillige Bestellung erfolgen darf. Am Institut des Datenschutzbeauftragten, als elementare Säule einer betrieblichen Selbstkontrolle[4], ist auch unter einem einheitlichen europäischen Gesetzesrahmen festzuhalten.

3 Gesetzliche Anreize in einer EU-DS-GVO

Der durch die GDD mitgegründete europäische Datenschutz-Dachverband „Confederation of Data Protection Organisations" (CEDPO) hat in seinem Positionspapier aus dem Jahre 2013 „Improve the protection of (our/your) data: 6 incentives for appointment of DPOs"[5] bereits auf mögliche Anreize für die Bestellung eines Datenschutzbeauftragten, die nicht ausschließlich auf gesetzlicher Basis ruhen, hingewiesen. Die GDD möchte die jüngsten Entwicklungen zum Anlass nehmen, auf einzelne dieser Anreize und deren Verankerung in einer EU-DS-GVO nochmals hinzuweisen.

Datenschutz-Folgenabschätzung und vorherige Zurateziehung (Art. 33 und 34 EU-DS-GVO)

Wie es auch das europäische Parlament in seiner legislativen Entschließung bereits vorgesehen hat[6], sollten Fragen einer verantwortlichen Stelle nach der Vereinbarkeit einer Verarbeitung personenbezogener Daten mit der EU-DS-GVO zunächst mit dem Datenschutzbeauftragten – falls durch das Unternehmen bestellt – als sachkundiger innerbetrieblicher Anlaufstelle geklärt werden können, bevor eine Hinzuziehung der zuständigen Aufsichtsbehörde erfolgt. Dies sollte bereits in der für risikobehaftete Verarbeitungsvorgänge vorgesehenen Datenschutz-Folgenabschätzung ausdrücklich normiert sein. Die seitens des Rats gewünschte beratende Funktion des Datenschutzbeauftragten (vgl. Art. 37 Abs. 1 (f)) reicht hierfür nicht aus, zumal die Entscheidung über die Konsultation der Aufsichtsbehörde letzten Endes der verantwortlichen Stelle übertragen wird, obwohl in Person des Datenschutzbeauftragten eine fachkundige Instanz bereits vorhanden wäre. Seine aktive Einbeziehung würde zur Entbürokratisierung von Datenschutzorganisation und -kontrolle beitragen. Betroffene würden von der Zurateziehung ebenfalls profitieren, da der Beauftragte die unternehmensinternen Abläufe kennt und entsprechend eine passgenaue Einschätzung äußern kann.

Sicherheitsvorfall (Art. 31 EU-DS-GVO)

Der Ratsentwurf sieht in Art. 31 Abs. 1 eine Informationspflicht der Aufsichts-

behörden im Falle der Verletzung des Schutzes personenbezogener Daten vor, sollte diese ein hohes Risiko für die persönlichen Rechte und Freiheiten von Betroffenen zur Folge haben. Die Europäische Kommission und das Parlament möchten gar, dass die Aufsichtsbehörden bei jeglicher Verletzung des Schutzes personenbezogener Daten informiert werden.[7] Um zu gewährleisten, dass Aufsichtsbehörden sich auch weiterhin ihren Kernaktivitäten in Gestalt der Beratung, Untersuchung und Kontrolle widmen können, sollten Datenschutzverstöße geringeren Umfangs, so beispielsweise der Verlust einer geringen Anzahl von Stammdatensätzen, ausschließlich durch den Filter des Datenschutzbeauftragten laufen können, damit dieser mögliche nachteilige Auswirkungen für die Rechte und Interessen Betroffener analysieren kann. Eine Information der Aufsichtsbehörde soll dann unterbleiben können, wenn der Datenschutzbeauftragte die Rechte und Interessen Betroffener unter Einhaltung der in Art. 31 vorgesehenen Maßnahmen als nicht weiter gefährdet sieht. Durch die zwingend vorgeschriebenen Dokumentationspflichten im Falle eines aufgetretenen Sicherheitsvorfalls ist es den Aufsichtsbehörden jederzeit möglich zu prüfen, ob und unter welchen Parametern die Untersuchung eines Vorfalls von statten gegangen ist und welche Maßnahmen hieraus abgeleitet wurden.

Zertifizierung (Art. 39 EU-DS-GVO)

Bestrebungen zur Stärkung datenschutzrechtlicher Gütesiegelverfahren sind bei allen Beteiligten des Trilogs erkennbar. Die Bestellung eines Datenschutzbeauftragten, der die Einhaltung der Vorgaben und Anforderungen einer EU-DS-GVO sicherstellt, sollte als Kriterium für besondere organisatorische Vorkehrungen in entsprechende Verfahren aufgenommen werden und die Vergabe eines höherrangigen Zertifikats ermöglichen. In Vorbereitung einer Siegelerlangung kann der Datenschutzbeauftragte durch seine Fachkunde die verantwortliche Stelle über angemessene technisch-organisatorische Maßnahmen im Sinne der EU-DS-GVO beraten und damit die Erlangung eines Gütesiegels beschleunigen.

Verwaltungsrechtliche Sanktionen (Art. 79 EU-DS-GVO)

Aufsichtsbehörden sollen nach Art. 79 der Entwürfe von Parlament und Kommission bzw. ergänzend nach Art. 79a des Ratsentwurfs befugt sein, verwaltungsrechtlichen Sanktionen zu verhängen. Diese müssen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein. Das Vorhandensein eines Datenschutzbeauftragten, als Zeichen dafür, dass Unternehmen den Schutz personenbezogener Daten ernst nehmen, sollte sich bei der Verhängung von Sanktionen bußgeldmildernd auswirken können. Immerhin hat die verantwortliche Stelle vorab bei der Verarbeitung personenbezogener Daten eine interne Kontrollinstanz um deren Einschätzung bemüht und sich entsprechenden fachlichen Rat eingeholt. Dies sollte bei der Verhältnismäßigkeit der Sanktionsmaßnahme entsprechend berücksichtigt werden können, vorausgesetzt die verantwortliche Stelle hat sich auch an der Empfehlung des Datenschutzbeauftragten orientiert.

4. Schlussbemerkungen

Die Beteiligten des Trilogs für eine EU-DS-GVO haben weiterhin die einmalige Gelegenheit, dem Datenschutzbeauftragten als Modell einer betrieblichen bzw. behördlichen Selbstkontrolle eine europäische Dimension auf gesetzlicher Grundlage zu verleihen. Gründe hierfür wurden bereits zur Genüge genannt. Doch selbst bei einer Abkehr von der Bestellpflicht hat der europäische Gesetzgeber noch genügend Möglichkeiten, im Rahmen des Trilogs Unternehmen wie Behörden bedeutende Anreize für eine freiwillige Bestellung zu bieten. Nur so kann gewährleistet werden, dass das Erfolgsmodell des Datenschutzbeauftragten auch unter einem neuen Gesetzesrahmen seine Bedeutung behält.

1 Vgl. Art. 35 Abs. 1 KOM(2012) 11 endgültig.

2 Vgl. Art. 35 Abs. 1 der legislativen Entschließung des Parlaments, abrufbar unter http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//DE.

3 So bspw. Polen und die Slowakei.

4 Hierzu bereits die Stellungnahme der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. zum Vorschlag für eine EU-Datenschutz-Grundverordnung (DS-GVO-E) vom 25.01.2012 (KOM(2012) 11 endgültig) hinsichtlich der Auswirkungen auf die Privatwirtschaft. abrufbar unter https://www.gdd.de/aktuelles/news/stellungnahme-der-gdd-zum-vorschlag-fur-eine-eu-datenschutz-grundverordnung-ds-gvo-e.

5 Abrufbar unter www.cedpo.eu.

6 Art. 34 Abs. 2 DS-GVO-E Parlament.

7 Kritisch hierzu bereits Stellungnahme der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. zum Vorschlag für eine EU-Datenschutz-Grundverordnung a.a.O., II. 14.

Aufgaben und Ziele der GDD e.V.

Die GDD tritt als gemeinnütziger Verein für einen sinnvollen, vertretbaren und technisch realisierbaren Datenschutz ein. Sie hat zum Ziel, die Daten verarbeitenden Stellen, insbesondere auch deren Datenschutzbeauftragte, bei der Lösung und Umsetzung der vielfältigen mit Datenschutz und Datensicherung verbundenen technischen, rechtlichen und organisatorischen Fragen zu beraten. Die GDD findet die Unterstützung von rund 2.500 Unternehmen, Behörden und persönlichen Mitgliedern. Sie stellt damit die größte Vereinigung ihrer Art und zugleich einen der größten Fachverbände in der Informations- und Kommunikationsbranche dar.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder
Michael Ronellenfitsch / Angelika Schriever-Steinberg / Nina Berg

Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen zur Datenschutz-Grundverordnung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich seit der Präsentation der Vorschläge durch die Kommission im Januar 2012 mehrfach öffentlich zur Datenschutzreform positioniert. Die folgende Zusammenfassung enthält einige der wichtigsten Themen, denen sich nach Ansicht der Konferenz der Datenschutzbeauftragten des Bundes und der Länder die am Trilog teilnehmenden Parteien insbesondere widmen sollten:

1. Keine Beschränkung des Anwendungsbereichs der Datenschutz-Grundverordnung

Die Beschränkung des Anwendungsbereichs der DSGVO zugunsten der JI Richtlinie sollte rückgängig gemacht werden. Die Datenverarbeitung der Ordnungsverwaltung und zur Gefahrenabwehr sollte von der DSGVO geregelt werden.

Aus dem Anwendungsbereich der DSGVO sollten nur solche Verarbeitungsvorgänge herausgenommen werden und damit ungeregelt bleiben, die sich ausschließlich auf persönliche und familiäre Tätigkeiten beziehen.

2. Datensparsamkeit muss Gestaltungsziel bleiben

Für eine möglichst grundrechtsschonende Datenverarbeitung ist es unabdingbar, dass sich Staat und Wirtschaft auf das zur Erreichung ihrer rechtlichen oder legitimen Zwecke notwendige Maß beschränken. Die allgegenwärtige Datenverarbeitung und der Einsatz von Big-Data-Technologien erzeugen eine unvorstellbare Menge an (auch personenbezogenen) Daten. Dies führt zu einer für viele als diffus bedrohlich empfundenen Situation, da auf diese Weise Unternehmen oder Behörden potentiell in der Lage sind, über jeden Einzelnen Informationen aus sämtlichen Lebensbereichen zu erfassen und beliebig auszuwerten. Deshalb ist das Prinzip von Datenvermeidung und Datensparsamkeit, das seit vielen Jahren im deutschen Datenschutzrecht verankert ist, wichtiger denn je.

Das Prinzip der Datensparsamkeit ist deshalb wie von Kommission und Parlament vorgesehen (Art. 5 Abs. 1 c) DSGVO) und leider vom Rat gestrichen ausdrücklich in der DSGVO zu verankern.

3. Keine Aufweichung der Zweckbindung

Die Zweckbindung ist seit jeher eines der zentralen Prinzipien des Datenschutzrechts. Sie dient der Transparenz und Vorhersehbarkeit der Verarbeitung personenbezogener Daten und stärkt damit die Autonomie der Betroffenen. Angesichts der Unsichtbarkeit und des Umfangs der Datenverarbeitung muss sich der Betroffene darauf verlassen können, dass seine personenbezogenen Daten grundsätzlich nur zu den Zwecken weiterverarbeitet werden, zu denen sie erhoben worden sind. Art. 8 Abs. 2 der Europäischen Grundrechtecharta hat daher die Zweckbindung als tragendes Prinzip des Datenschutzes verankert. Durch die Formulierungen der Kommission und des Rats werden Zweckänderungen in einem derart weiten Umfang zulässig, dass das für den Datenschutz elementare Prinzip der Zweckbindung preisgegeben wird. Es sollte deshalb dem Vorschlag des Parlaments gefolgt werden, der diese Zweckänderungen nicht vorsieht.

4. Die Einwilligung muss die Datenhoheit des Einzelnen sichern

Die Einwilligung ist ein wesentliches Element, um die Autonomie des Einzelnen hinsichtlich der Verarbeitung seiner personenbezogenen Daten wirksam zu sichern. Sie ist deshalb in Art. 8 Abs. 2 der EU-Grundrechtecharta ausdrücklich als Legitimation für die Verarbeitung personenbezogener Daten genannt.

Kommission und Parlament haben sich im Bewusstsein dieser Bedeutung dafür entschieden, dass eine Einwilligung nur dann wirksam sein soll, wenn sie ausdrücklich erfolgt. Der Rat verabschiedet sich von diesem Grundsatz, indem er bereits eine eindeutige und damit auch nur konkludente Willensbekundung ausreichen lässt. Damit wird es insbesondere den global agierenden Diensteanbietern ermöglicht, durch die Verwendung pauschaler Datenschutzbestimmungen und datenschutzunfreundlicher Voreinstellungen weitreichende Datenverarbeitungsbefugnisse ohne eine ausdrückliche Einwilligung des Nutzers für sich zu reklamieren. Es muss deshalb dabei bleiben, dass eine Einwilligung nur dann die Verarbeitung personenbezogener Daten legitimieren kann, wenn sie ausdrücklich abgegeben wird.

5. Rechte der Betroffenen

Die Information der Betroffenen (Art. 14, 14a DSGVO) versetzt diese in die Lage, Umfang und Risiko der Datenverarbeitung einzuschätzen. Sie ist die wesentliche Bedingung für die Schaffung von Transparenz. Der Umfang dieser Informationen dürfen nicht – wie vom Rat vorgesehen – eingeschränkt werden.

Es sollte unmissverständlich klargestellt werden, dass die Ausübung der Betroffenenrechte und deren Umsetzung unentgeltlich ist.

Die bisherigen Vorschläge von Kommission, Parlament und Rat für eine

Regelung von Profilbildungen (Art. 20 DSGVO) sind nicht geeignet, um die Bürgerinnen und Bürger im Zeitalter von Big Data, der Allgegenwart des Internets der Dinge und der in alle Lebens-, Privat- und Intimbereiche wie die Gesundheit vordringenden Technologien zur individuellen Datenerfassung und -analyse effektiv vor der Erstellung und Nutzung von Persönlichkeitsprofilen zu schützen.

Keiner der Vorschläge unterwirft die Profilbildung an sich besonderen Zulässigkeitsvoraussetzungen sondern erst das Treffen einer „automatisierten Entscheidung“ oder einer „Maßnahme“ auf Basis des Profilings. Nicht geregelt wird die grundlegende Frage, zu welchen Zwecken und innerhalb welcher Grenzen Persönlichkeitsprofile überhaupt erstellt und genutzt werden dürfen. Zudem beinhaltet dieser Ansatz in der Praxis ein erhebliches Interpretations- und Umgehungspotenzial im Hinblick auf Dienste oder Anwendungen, die keine unmittelbaren Rechtswirkungen gegenüber dem Betroffenen entfalten, wie die Analyse des Nutzerverhaltens im Internet, die Analyse persönlicher Vorlieben durch ein soziales Netzwerk, die Analyse von Bewegungsdaten oder die Analyse der Körperaktivität mittels Apps und Sensoren.

Anzustreben ist eine substanzielle Verbesserung der Regelung der Profilbildung und -nutzung, die folgende Kernelemente beinhalten sollte:

- Statt der Verkürzung auf automatisierte Einzelfallentscheidungen ist ein Ansatz zu wählen, der sämtliche Profilbildungen oder darauf basierende Maßnahmen erfasst.

- Ausnahmen vom Verbot der Profilbildung bedürfen eng begrenzter klarer Erlaubnistatbestände. Besondere Kategorien personenbezogener Daten dürfen wegen ihrer hohen Sensitivität nicht in eine Profilbildung einfließen.

  In jedem Fall sollte die Verarbeitung personenbezogener Daten zu Zwecken des Profilings stets mit einem Höchstmaß an Transparenz und Informiertheit des Betroffenen einhergehen. Der Einzelne muss hierzu seine ausdrückliche Einwilligung erteilen.

- Zudem sollte eine Verpflichtung zu frühestmöglicher Anonymisierung oder Pseudonymisierung der für die Profilbildung und -auswertung verwendeten Daten bestehen.

6. Guter Datenschutz braucht betriebliche und behördliche Datenschutzbeauftragte

Es ist zu begrüßen, dass sowohl Kommission als auch Parlament (Art. 35 DSGVO) – anders als der Rat – die verpflichtende Bestellung interner Datenschutzbeauftragter vorsehen. Während es für Behörden keine Ausnahmen geben sollte, sollten Unternehmen nicht nur ab einer bestimmten Größe oder einer bestimmten Zahl Betroffener einen Datenschutzbeauftragten bestellen, sondern in jedem Falle auch dann, wenn die Datenverarbeitung mit besonderen Risiken für die Rechte und Freiheiten der Betroffenen verbunden ist.

7. Mehr Kontrolle über Datenübermittlungen an Behörden und Gerichte in Drittstaaten

Seit den Enthüllungen von Edward Snowden wird über einen besseren Schutz der personenbezogenen Daten von europäischen Bürgerinnen und Bürgern gegenüber Behörden und Stellen aus Drittstaaten diskutiert. Deshalb hat das Parlament einen spezifischen Art. 43a DSGVO vorgeschlagen, der vom Rat leider gestrichen wurde. Dieser stellt klar, dass Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden eines Drittstaats, die die Weitergabe personenbezogener Daten an diesen verlangen, in der EU nur unter besonderen Voraussetzungen durchgesetzt werden können. Eine derartige Regelung könnte in einem gewissen Umfang Transparenz über das Ausmaß der Überwachung durch Geheimdienste herstellen, zur Wahrung der Verhältnismäßigkeit beitragen, Anreize zur Verabschiedung internationaler Übereinkommen schaffen und sollte deshalb getroffen werden.

8. Für eine effektive und bürgernahe Zusammenarbeit der Datenschutzbehörden in Europa

Ein entscheidender Fortschritt der Datenschutz-Grundverordnung soll in einer verbesserten Zusammenarbeit der Datenschutzbehörden in Europa liegen. Auf Vorschlag des Rats soll es eine federführende Datenschutzbehörde geben, die einem Unternehmen am Ort seiner Hauptniederlassung als hauptsächlicher Ansprechpartner zur Verfügung steht, aber auch mit allen anderen – sei es aufgrund weiterer Niederlassungen oder der Betroffenheit ihrer Bürger – betroffenen Aufsichtsbehörden kooperiert. Weiterhin hat der Rat Vorschläge zu einem sog. One-Stop-Shop gemacht, sodass Betroffene sich an die Aufsichtsbehörde und die Gerichte bei ihnen vor Ort wenden können. Um zu verbindlichen Entscheidungen ohne Beteiligung der Kommission zu kommen, schlägt der Rat darüber hinaus vor, den Europäischen Datenschutzausschuss mit verbindlichen Entscheidungsbefugnissen auszustatten. Hierzu ist der Ausschuss mit eigener Rechtspersönlichkeit auszustatten.

Die Ziele des Ratsvorschlags zum sog. One-Stop-Shop-Mechanismus sind zu unterstützen. Der effiziente Vollzug des Datenschutzrechts darf jedoch nicht durch die Untätigkeit der federführenden Datenschutzbehörde unterlaufen werden. Es ist eine Regelung zu schaffen, wonach die mitgliedstaatlichen Aufsichtsbehörden bei Betroffenheit ihrer Bürger von der federführenden Behörde ein aufsichtsbehördliches Einschreiten verlangen können, dessen Ablehnung zu einer unmittelbaren Überprüfung durch den Europäischen Datenschutzausschuss führt. Darüber hinaus sind praktikable Verfahrensregeln festzulegen, insbesondere was die Frage der Verfahrensfristen und der Amtshilfe der Aufsichtsbehörden untereinander betrifft.

Autoren dieses Beitrages sind:
Prof. Dr. Michael Ronellenfitsch
Angelika Schriever-Steinberg
Nina Berg

Douwe Korff *

Privacy seals in the new EU General Data Protection Regulation: Threat or facilitator? †

In 2008, the European Commission helped to establish the currently main scheme offering European privacy- or data protection seals (certifications), *EuroPriSe*, under an "eTEN" programme. The Commission's draft of the General Data Protection Regulation (hereafter: "the Regulation"), made public in January 2012, requires the Commission itself and the Member States to further "encourage" the establishment of such schemes, "in particular at European level" (Art. 39).

However, *EuroPriSe* has had only limited success, mainly because it (rightly) sets very high standards and is thus very demanding of seal applicants in terms of time and effort and costs – yet under the current 1995 EC Data Protection Directive, it cannot offer any concrete legal advantages to those meeting those standards. It is also seriously hampered by the lack of harmonisation under the directive: it can provide an authoritative (albeit non-legally-binding) confirmation of compliance with the rules in the EC directives (the 1995 Directive, the 2002 e-Privacy Directive and the [now invalidated] Data Retention Directive), but not of compliance with the dozens of national laws implementing those laws. It is therefore really only attractive to companies that want to make privacy- and data protection compliance a major "unique selling point" for their products and services. Regrettably, those are scarce. It is notable that the much more geographically limited privacy seal in the small German state of Schleswig-Holstein, which under the local state (*Landes-*) data protection law does offer concrete advantages, in particular in relation to public procurement, has attracted more seal applications than the in principle pan-EU/EEA *EuroPriSe* scheme.

Although the Regulation will lead to much greater harmonisation, and in particular contains a "consistency mechanism" as discussed below, this alone will not, in my opinion, lead to a major increase in seal applications. For that, stronger incentives are crucial.

I therefore welcomed the European Parliament proposals to give data protection seals ("certifications") a much stronger role – subject to crucial conditions. Specifically, its amended draft of Article 26(3a) of the Regulation stipulates expressly (with cross-reference to Art. 26(1)) that "certification mechanisms" can in and by themselves "demonstrate" that a processor:

> provid[es] sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject ... -

and its amended draft of Article 42 similarly stipulates that "a valid 'European Data Protection Seal'" can in and by itself "demonstrate" that a controller has adopted "appropriate safeguards" to allow data to be transferred to a "third" (i.e., non-EU/EEA) country that does not itself provide "adequate safeguards" in its laws (provided the seal applies both to the controller and to the intended recipient(s) in the third country) (EP Amendment 138).

In practice, seals could also serve to show compliance with other, more general requirements that, under the Regulation, in future will need to be "demonstrated" (cf., e.g., Articles 19, 32, 33, etc.)

These would be very significant advantages to seal holders. In particular, European privacy seals that would allow data transfers (also) to the USA, and to processors in the USA (such as U.S. "Cloud" providers), could come to replace the discredited "Safe Harbor" regime, rightly condemned by the European Parliament and under review by the Commission.

However, if seals were indeed to be endowed with such considerable legal effects, they would have to be based on the application of very high standards – and those standards would have to be applied consistently in all schemes established under Article 39 of the Regulation, and at least implicitly endorsed by all DPAs and the newly-to-be-established European Data Protection Board (EDPB).

In my opinion – and in the opinion of civil society[1] – this means two things:

- seals that have legal effects such as noted above (i.e., which "demonstrate" compliance with important requirements of the Regulation, not least the rules on data transfers) should be issued by an official data protection authority ("supervisory authority" in the terminology of the Regulation);
AND
- such seals should be subject to the "consistency mechanism" envisaged in the Regulation, under which many "measures" taken by any DPA which are "intended to produce legal effects" can be challenged by any other DPA and brought to the new European Data Protection Board (composed of representatives of all EU/EEA DPAs) – which could decide, at the European level, whether the proposed measure (in casu: the issuing of a seal) should or should not go ahead. This consistency mechanism will apply, *inter alia*, to

> processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour [typically, in relation to only activity by the data subjects]

As the above already makes clear, the two are interlinked, in that the consistency mechanism applies whenever a DPA

wishes to adopt measures with legal effects that also affect data subjects in other Member States.

The European Parliament text achieves the above, by **(i)** stipulating that seals (certifications) must be issued by a DPA (Art. 39(1a) in the EP draft); **(ii)** as noted above, giving seals important legal effects; and **(iii)** thus, automatically, making the issuing of seals relating to processing of personal data in more than one Member State or online subject to the consistency mechanism.

However, the last Council version of the Regulation, agreed just before the summer break, would fatally undermine the above. In particular, it allows Member States to "outsource" the issuing of seals to "accredited" organisations. Although organisations could only be accredited if they met certain standards set at EU level, crucially the seals they issued would **not** need to be formally endorsed by the relevant DPA (See Art. 39 in the latest Council text). This in turn would mean that the issuing of a seal would **not** constitute a "measure with legal effect", taken by a DPA – and would thus also **not** be subject to the consistency mechanism. Interestingly, precisely such an "outsourced" data protection seal system is being planned by the UK DPA, the Information Commissioner's Office, for later in 2015 or early-2016.

Yet although data protection seals issued under the Council text would not be subject to the consistency mechanism, they would, under that text, still be given at least some of the legal advantages envisaged in the European Parliament text – if anything in more emphatic terms. In particular, in the Council version, a controller can provide "appropriate safeguards" for a transfer of data to a third country without adequate protection "**without requiring any specific authorisation from a supervisory authority**", by means, inter alia of:

> an approved certification mechanism pursuant to Article 39
> (Art. 42 Council text)

Although the Council text does require that such seals be accompanied by:

> enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights –

these "enforceable commitments" would, of course, only relate to the commitments required under the relevant seal – which some other DPAs might find insufficient. However, since under this text the seal would not be issued by a DPA, and thus does not constitute a "measure with legal effects" on the part of the DPA, the appropriateness of the awarding of the seal itself (and the adequacy or otherwise of any such requirements and "commitments" as may – or may not – be specified in the seal) could not be challenged by any other DPA.

In my opinion – and in the opinion of civil society – this Council proposal amounts to the rolling in of a massive Trojan Horse into the new EU data protection regime.

It would allow transfers of personal data – including highly sensitive personal data – from the EU/EEA to the USA and other "third" countries that do not provide "adequate protection" (including to "Cloud" providers in such countries), from an EU/EEA country with an "outsourced" data protection seal system (such as is planned in the UK), without the data protection authorities in any other EU/EEA country being able to challenge the transfers.

It would moreover encourage a "race to the bottom" for seal providers keen to attract major international – and in particular U.S. – applicants for their seals. The easier their seals could be obtained, the more attractive they would be to non-EU/EEA controllers and processors.

This is unacceptable.

In simple terms: there is a choice of systems:

> either the Regulation allows for "outsourced" European data protection seals – but without such seals conferring any real legal benefits on seal holders (which would not make them much more attractive then the current EuroPriSe seals),
> **OR**
> the Regulation facilitates the establishment of strong European data protection seal schemes, at national and/or European level (and they could be sectoral too), with those seals conferring real legal benefits to seal holders, in particular by allowing them, without further ado, to operate as a "processor" and/or to transfer data to third countries without adequate protection – **but only** if the seals were, if not actually issued by, at least formally endorsed by a national DPA, meaning that they would constitute "measures with legal effects" of the DPA in question, and that they would be subject to the consistency mechanism.

In his latest comments on the Regulation (and in particular on the last Council text), the European Data Protection Supervisor appears to choose the first option, by proposing to simply remove seals (certifications) from Article 42 as a means to demonstrate "adequate protection" for data transfers.[2] It may be that he feels that is the saver choice.

However, the latter option would ensure that seals would only be issued to internationally operating companies, including Internet companies, if all the European DPAs agreed, in the new EDPB, that a seal was appropriately awarded, and did not in any way undermine the fundamental rights and freedoms, and in particular the data protection rights and freedoms, of European citizens (at least in the sense that none would feel the need to challenge a proposed seal). In my opinion, such strong seals, tested in the consistency mechanism if necessary, would bring real benefit to industry and data subjects alike.

I therefore strongly urge those involved in the "trilogues" on the Regulation that are now starting, to adopt this latter option, and to reject in particular the Council proposals which would undermine the rights and freedoms of our citizens.

It is perhaps worthy of note that at the conference where I first presented the above,† the vast majority of participants, who mainly came from global industry, when expressly asked, supported the second option for strong seals issued by DPAs, over and above the first one.

Finally, I should add that this does not necessarily mean that a country could

not choose to effectively "outsource" the heavy, frontline work involved in the (quite laborious) evaluation of products and services put forward for a seal. On the contrary, that work can very well be done by separately established but appropriately vetted – i.e., accredited – independent bodies including bodies established by the private sector (such as *EuroPriSe* itself now is). But the evaluations carried out by them would have to be checked by the relevant DPA, and a seal should not be issued unless it is at least (if it is not issued directly by a DPA) formally endorsed by the relevant DPA in the form of an "act with legal effects" (German: *Verwaltungsakt*).

Douwe Korff
Cambridge, August 2015

* Douwe Korff is Emeritus Professor of International Law, London Metropolitan University; an Associate of the Oxford Martin School of the University of Oxford (Member of the Expert Advisory Panel of the OMS Global Cybersecurity Capacity Centre); and a Fellow of the Centre for Internet & Human Rights of the University of Viadrina, Frankfurt/O and Berlin. He helped to establish the "European Privacy Seal" (EuroPriSe) scheme under an EC "eTEN" programme in 2008 and has been a EuroPriSe expert since, evaluating a range of products offered by ValidSoft UK Ltd, all relating to fraud prevention by financial institutions.

† This article is partly based on a presentation by the author to the 5th European Data Protection Days Euroforum conference in Berlin, 4 – 5 May 2015.

Notes:

1 On 11 August 2015, the EuroPriSe website listed 35 seals as having been issued (not counting re-certifications required every two years):

https://www.european-privacy-seal.eu/EPS-en/Awarded-seals

By the same day, the Schleswig-Holstein data protection authority, ULD, had (since 2009) issued 38 seals:

https://www.datenschutzzentrum.de/guetesiegel/register/2009-2013/

Other European schemes, such as the recently-introduced French system of "Labels" issued by the French data protection authority, the CNIL, are more limited and not really comparable to the above-mentioned German schemes. Under the German schemes, any company can apply for a seal for any (IT) product or service, while under the French scheme, companies can to date only certify compliance with a few pre-specified sets of standard requirements for very specific products or services (to date: data protection audits; data protection training; [arrangements for internal] data governance; and [cloud] data "vaults"):

http://www.cnil.fr/linstitution/labels-cnil/

2 Annex to Opinion 3/2015, Europe's big opportunity – EDPS recommendations on the EU's options for data protection reform, 27 July 2015, containing a Comparative table of GDPR texts with EDPS recommendations (see the texts for Article 42):

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_Annex_EN.pdf

Peter Schaar
Europäische Akademie für Informationsfreiheit und Datenschutz, Bundesbeauftragte für Datenschutz und Informationsfreiheit a.D.

Europäischer Datenschutz: Bitte nicht aufweichen!

Die von der Europäischen Kommission vor mehr als drei Jahren auf den Weg gebrachte Datenschutzreform ist zwar noch nicht in „trockenen Tüchern", aber immerhin ist absehbar, dass zumindest die Datenschutz-Grundverordnung in absehbarer Zeit von den EU-Gremien beschlossen wird. Bei allen Unsicherheiten im Detail bietet sich damit die einmalige Chance, Herausforderungen an das Datenschutzrecht in Angriff zu nehmen und diese mit einer stärkeren europäischen Harmonisierung zu verbinden. Gerade die Kombination dieser beiden Aspekte macht den möglichen Charme der Reform aus. Dies gilt freilich nur, wenn die Harmonisierung auch zu einem möglichst hohen Datenschutzstandard führt und nicht bloß einen kleinsten gemeinsamen Nenner definiert.

Positiv anzumerken ist, dass wesentliche Grundelemente der Datenschutzreform zwischen den EU-Gremien unstreitig sind: Die Einbeziehung von Unternehmen aus Drittstaaten, die in Europa aktiv sind (Marktortprinzip), den Abbau des Datenschutzgefälles zwischen den Mitgliedstaaten und – last but not least – die Stärkung der Datenschutzaufsicht.

Trotzdem gibt es keinen Anlass, sich beruhigt zurückzulehnen und den Ausgang des Trilogs zwischen Kommission, Parlament und Rat abzuwarten. Zum einen haben die Bemühungen von Interessenvertretungen erneut zugenommen, denen die ganze Richtung nicht passt. Bedauerlich ist insbesondere, dass auch manche europäischen Industrievertreter noch nicht verstanden haben, dass ein wirksamer, europaweit harmonisierter Datenschutz in ihrem wohlverstandenen wirtschaftlichen Interesse liegt. Zum anderen gibt es durchaus auch in den EU-Gremien Neigungen, dem Druck solcher Unternehmen – vor allem aus Drittstaaten – nachzugeben, deren Geschäftsmodelle kaum mit einem hohen europäischen Datenschutzniveau kompatibel sind. Zwar ist das Europäische Parlament in seiner Positionsbestimmung überwiegend zu Gunsten des Datenschutzes über den Kommissionsentwurf hinaus gegangen. Dagegen enthält

die Richtungsentscheidung des Rats gefährliche Aufweichungen und bleibt sogar an verschiedenen Punkten hinter dem derzeitigen Recht zurück.

Für den Trilog sind insbesondere die folgenden Felder wichtig, in denen – teils erhebliche – Meinungsdivergenzen zwischen den Gremien bestehen. Im Sinne eines wirksamen Datenschutzes müssen hier klare Weichenstellungen getroffen werden:

- Keine Aufweichung der **Zweckbindung**. Eine generelle Erlaubnis für Unternehmen oder Behörden, bei „überwiegendem Interesse" Daten auch für Zwecke zu verwenden, die mit dem Erhebungszweck nicht vereinbar sind, wäre mit der Gewährleistung des Grundrechts auf Datenschutz nicht vereinbar.

- Die Bürgerinnen und Bürger müssen wirksam vor der Zusammenführung ihrer Daten zu **Persönlichkeitsprofilen** geschützt werden. Profiling sollte grundsätzlich nur unter Pseudonym zulässig sein, wobei die Pseudonyme möglichst robust und rücknahmefest zu konstruieren sind. Auch bei der Verwendung von Pseudonymen muss der Betroffene umfassend über die Tatsache und die Zwecke des Profiling informiert werden und ihm ggf. widersprechen können. Sensible Daten sollten generell vom Profiling ausgenommen werden. Für den Betroffenen nachteilige, auf automatisierten bzw. überwiegend auf automatisierten Verfahren beruhende Einzelentscheidungen sollten unzulässig sein.

- Der **Datentransfers in Drittstaaten** sollte generell nur zulässig sein, wenn ein angemessenes Datenschutzniveau vorliegt, das den Anforderungen der EU-Grundrechtecharta genügt. Gerade die im wesentlichen auf Edward Snowden zurückgehenden Veröffentlichungen über umfassende geheimdienstliche Überwachungsmaßnahmen haben gezeigt, dass die bisherigen Instrumente defizitär sind. Die vom Rat vorgeschlagenen Ausnahmeregelungen für bestehende Adäquanzentscheidungen, etwa für Safe Harbor, im Rahmen von bilateralen Abkommen oder für Verwaltungsvereinbarungen zwischen öffentlichen Stellen wären inakzeptabel.

- **Sektorspezifische nationale Regelungen** – etwa zum Gesundheitswesen und zum Beschäftigtendatenschutz – dürfen das durch die GVO festgelegte Mindestniveau des Datenschutzes nicht unterschreiten. Dagegen sollte es den Mitgliedstaaten weiterhin möglich sein, in begründeten Fällen, insb. bei der Verarbeitung sensibler Daten, aber auch bei der behördlichen Datenverarbeitung, weitergehende Schutzvorschriften vorzusehen, damit durch nationales Verfassungsrecht (z.B. durch die Rechtsprechung des Bundesverfassungsgerichts) garantierte Standards auch weiterhin gewährleistet werden können.

- Die Verarbeitung personenbezogener Daten auf Basis einer **Einwilligung** sollte nur zulässig sein, wenn die faktische Freiwilligkeit gewährleistet ist. Im Falle gravierender Machtunterschiede zwischen der verantwortlichen Stelle und dem Betroffenen kann im Regelfall nicht hiervon ausgegangen werden. Die Einwilligung sollte generell ausdrücklich erfolgen und nicht implizit.

- Die für die Verarbeitung von Daten für **statistische** und für **Forschungszwecke** vorgesehenen weit reichenden Sonderregelungen müssen durch besondere Schutzvorkehrungen, insbesondere durch ein wirksames Forschungsgeheimnis, abgesichert werden.

- Der **technologische Datenschutz** sollte gestärkt werden. Dazu ist es erforderlich, die Vorgaben zu Privacy by Design, Privacy by Default und zur Datenschutzfolgenabschätzung konkreter und verbindlicher zu fassen. Die Vorgaben zur Vergabe und Verwendung qualifizierter Datenschutz-Gütesiegel sollten verbindlicher formuliert werden.

- Die unabhängigen **Datenschutzaufsichtsbehörden** brauchen wirksame Sanktionsmöglichkeiten bei Verstößen, die sich an der wirtschaftlichen Leistungsfähigkeitr der Unternehmen orientieren. Angesichts der erheblichen, mit der GVO verbundenen Ausweitung ihrer Aufgaben benötigen sie eine angemessene personelle und sachliche Ausstattung nach einem europaweit verbindlichen Standard. Der aus den Aufsichtsbehörden gebildete Datenschutzausschuss sollte über Streitfragen über die Auslegung der GVO verbindlich entscheiden. Eine Letztentscheidungsbefugnis der Kommission wäre damit unvereinbar.

- Die Bestellung **interner** (betrieblicher/behördlicher) **Datenschutzbeauftragter** sollte in der gesamte EU obligatorisch sein. Ihre unabhängige Stellung sollte rechtlich effektiv abgesichert sein, etwa durch entsprechenden Kündigungsschutz.

vzbv – Florian Glatzner

Datenschutz in Europa: Die roten Linien des vzbv

Die Digitalisierung berührt und verändert alle Lebensbereiche der Menschen. Schon heute lässt sich Vieles im Alltag ohne Internetzugang und -nutzung kaum noch bewerkstelligen. Vernetzte Geräte vereinfachen zwar das Leben der Verbraucher, erzeugen aber auch ständig Daten, hinterlassen bleibende Datenspuren und verknüpfen Daten zu verschiedenen – individuell nicht steuerbaren – Aussagen und Prognosen. Die geltende Europäische Datenschutzrichtlinie von 1995 erfasst viele Probleme des Datenschutzes nicht, mit denen Verbraucherinnen und Verbraucher heute konfrontiert sind. Eine Modernisierung der gesetzlichen Regelungen, ihre Anpassung an die Herausforderungen der der Gegenwart und Zukunft ist daher dringend notwendig. Es braucht klare Regeln, um den Schutz der persönlichen Daten und der Privatsphäre der Verbraucher gewährleisten zu können und gleichzeitig Rechtssicherheit und Wettbewerbsfähigkeit europäischer Unternehmen zu stärken. Die Novellierung der Datenschutzverordnung der Europäischen Union ist somit eines der wichtigsten Regulierungsinstrumente für die nächsten Jahre, wenn nicht Jahrzehnte.

Nach Ansicht des Verbraucherzentrale Bundesverbands e.V. (vzbv) hat sich aber die inhaltliche Diskussion während der zurückliegenden dreieinhalb Jahre schrittweise in eine datenschutzunfreundliche Richtung bewegt. Während die Europäische Kommission und das EU-Parlament ein Mehr an Datenschutz anstreben, ist durch die deutlich wirtschaftsfreundlichere Positionierung des Rates der Europäischen Union eine Situation für die weiteren Verhandlungen entstanden, wo es an vielen Stellen nur noch um den Erhalt des geltenden Niveaus auf europäischer und nationalstaatlicher Ebene gehen wird. Damit ist das Gesamtziel der so dringlichen Modernisierung der Richtlinie von 1995 gefährdet. Ziel war ein Mehr an Datenschutz und Datensicherheit, im Gespräch ist durchaus auch ein Weniger – eine Punktlandung soll nun sein, den gegenwärtigen Regelungsstand nicht zu unterbieten. Für Verbraucher kein Erfolg!

Rote Linien des vzbv beim europäischen Datenschutz

1. Datensparsamkeit

Ein Grundprinzip eines wirksamen Datenschutzes ist die Datensparsamkeit. Das Bundesdatenschutzgesetz beispielsweise regelt: „*Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen*."

Auf diese Weise sollen die Risiken der Datenverarbeitung verringert und deren Verhältnismäßigkeit gewahrt werden. Unternehmen müssen demnach stets kritisch prüfen, ob die zu verarbeitenden Daten tatsächlich nötig sind, oder ob nicht mit weniger (oder pseudonymisierten oder anonymisierten) Daten derselbe Zweck erzielt werden kann. Dadurch wird auch die Entwicklung und Anwendung datenschutzfreundlicher Technologien gefördert.

Nach den Vorschlägen des Rates der Europäischen Union aber sollte eine Datenverarbeitung künftig nicht mehr auf ein Minimum begrenzt werden, sondern lediglich „nicht exzessiv" sein. Dies würde aber eine deutliche Absenkung des geltenden Datenschutzniveaus bedeuten. Dieser Vorschlag des Rates ist somit inakzeptabel.

2. „Berechtigtes Interesse" der datenverarbeitenden Stelle

Die Rechtmäßigkeit der Verarbeitung kann durch „berechtigte Interessen" eines für die Verarbeitung Verantwortlichen begründet sein, sofern die Interessen oder Rechte Betroffener nicht überwiegen. Die Regelung darf aber nicht dazu führen, dass Unternehmen künftig Daten auf Basis eines Berechtigten verarbeiten, wenn sie beispielsweise keine Einwilligung der Betroffenen einholen möchten. Dementsprechend sollte eine Datenverarbeitung auf Grundlage einer Interessenabwägung nur erlaubt sein, wenn dies aus objektiven Gründen tatsächlich erforderlich ist (wovon man beispielsweise bei der Verwendung personenbezogener Daten zu Werbezwecken grundsätzlich nicht ausgehen kann).

Der vzbv hält es für unerlässlich, dass die Verordnung keine weite Auslegung des „berechtigten Interesses" zulässt. Der Rat der Europäischen Union fordert, eine Änderung des Verarbeitungszwecks auf Basis der Interessenabwägung auch dann zuzulassen, wenn keine Kompatibilität mit dem ursprünglichen Zweck der Datenerhebung besteht. Wird das „berechtigte Interesse" der Unternehmen an dieser Stelle zu weit gefasst, wäre die Zweckbindung faktisch aufgelöst.

Vor diesem Hintergrund kritisiert der vzbv, dass das Europäische Parlament und der Rat der Europäischen Union eine Datenverarbeitung zu Zwecken des Direktmarketings grundsätzlich vom „berechtigten Interesse" der datenverarbeitenden Stelle oder eines Dritten, an den die Daten weitergegeben wurden, gedeckt sehen. Die Positionen bleiben damit sogar hinter den in Deutschland aktuell geltenden Regelungen zurück.

Der vzbv fordert daher von der Europäischen Kommission, dem EU-Parlament und vom Rat der Europäischen Union klare Kriterien für eine enge Auslegung des „berechtigten Interesses". Insbesondere für die Nutzung von personenbezogenen Daten zu Werbezwecken sollte grundsätzlich eine Einwilli-

gung des Betroffenen eingeholt werden müssen.

3. Änderung des Verarbeitungszwecks

Auch das Prinzip der Zweckbindung ist einer der Grundpfeiler des Datenschutzes. Es ist in der EU-Grundrechtecharta verankert, nach der Daten *„nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden*“ dürfen. Auch die bisherige Europäische Datenschutzrichtlinie regelt, dass personenbezogene Daten nur *„für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden*“ dürfen.

Der Entwurf der Europäischen Kommission führt jedoch eine Regelung ein, nach der personenbezogene Daten auch bei nicht bestehender Kompatibilität mit dem ursprünglichen Zweck der Datenerhebung verarbeitet werden könnten, wenn ein sonstiger Rechtfertigungsgrund, z.B. eine Einwilligung oder vertragliche Grundlage, einschlägig ist. In seiner Positionierung spricht sich der Rat der Europäischen Union dafür aus, die Regelung sogar noch auf personenbezogene Daten auszuweiten, die auf Basis eines „berechtigten Interesses“ verarbeitet werden. Besonders in Verbindung mit der weiten Auslegung des Begriffs des „berechtigten Interesses“ in der Verordnung würde die Zweckbindung somit künftig aufgelöst.

Der vzbv hält grundsätzlich jede Weiterverarbeitung von personenbezogenen Daten, die nicht mit dem Zweck vereinbar ist, für die die Daten ursprünglich erhoben wurden, für äußerst kritisch. Eine solche Regelung bietet zu viele Spielräume für datenverarbeitende Stellen, Daten weiterzuverwenden und an Dritte zu übermitteln. Sie führt unweigerlich dazu, dass Verbraucher völlig unerwartet mit der weiteren Nutzung ihrer Daten konfrontiert würden. Dies zerstört Vertrauen der Verbraucher in die Wirtschaft, dass mit ihren Daten verantwortungsvoll und nach ihren Wünschen umgegangen wird. Für ein begründetes Vertrauen sind klare gesetzliche Begrenzungen der Datenverarbeitung, wie ein strikter Zweckbindungsgrundsatz, erforderlich.

4. Profilbildung

Mit der Digitalisierung werden systematisch immer mehr Informationen über Vorlieben, Ansichten und persönliche Verhältnisse der Verbraucher gesammelt und in Profilen zusammengefasst. Ziel ist die Vorhersehbarkeit und damit Steuerbarkeit menschlichen Verhaltens. Daten, die detaillierte Aufschlüsse über Motivationen, Präferenzen, Beziehungen, Gesundheit oder sonstige Faktoren des Selbstwerts einer Person geben, sind zu wertvollen marktfähigen Gütern geworden. Sie können entscheidend dafür sein, ob Verbraucher Kredite erhalten, welche Versicherungsbeiträge sie leisten müssen oder welche Preise sie für Güter bezahlen. Die Profilbildung hat nicht nur massive Auswirkungen auf den Einzelnen, sondern auch auf die Gesellschaft. Umso wichtiger ist eine verbraucherfreundliche Ausgestaltung der Profilbildung mit klaren Grenzen.

Daher muss die Profilbildung selbst begrenzt werden. Denn schon die reine Bildung eines Profils greift tief in die Rechte betroffener Personen ein. Auch darf eine Profilbildung nicht erst reguliert werden, wenn sie dem Verbraucher gegenüber eine rechtliche Wirkung entfaltet oder ihn in maßgeblicher Weise beeinträchtigt. Eine Profilbildung, die es ermöglicht, Verbrauchern individualisierte Werbung anzuzeigen oder Produkte und Dienstleistungen zu individuellen Preisen anzubieten, wäre ansonsten gar nicht erst durch die Verordnung erfasst. Zu diesen Zwecken wird die Profilbildung jedoch oft angewendet.

Die Verarbeitung personenbezogener Daten ist gerade in Hinblick auf die Profilbildung besonders kritisch. Daher sollte eine Profilbildung auch auf Grundlage besonderer Kategorien von personenbezogenen Daten nur unter strengen Bedingungen erlaubt sein.

Peter Wedde

Die EU-DS-GVO – Beschäftigtendaten-Verarbeitungs-Erlaubnisverordnung statt Beschäftigtendatenschutz?

In betrieblichen Datenverarbeitungssystemen findet sich heute eine Fülle personenbezogener Beschäftigtendaten. Dies ist keine neue Erkenntnis. Grundlegend neu sind aber die Verknüpfungs- und Auswertungsmöglichkeiten, die Arbeitgebern inzwischen zur Verfügung stehen. In Zeitalter von „Big Data“, „Industrie 4.0“ und „Unified Communication“ ist der „Gläserne Arbeitnehmer“ längst Realität. Die Durchsichtigkeit nimmt nochmals zu, wenn vorhandene betriebliche Daten mit privaten Informationen verknüpfen werden, die im Internet zur Verfügung stehen. Gleiches gilt für Bewerber, wenn die von ihnen an potentielle Arbeitgeber übergebenen Informationen mit Daten aus dem Internet verknüpft werden. Wer da Pech hat, wird schon im Vorfeld eines Erstgesprächs gnadenlos ausgesiebt. Ähn-

liches kann für ehemalige Beschäftigte gelten, die sich anderenorts bewerben.

Vor dem Hintergrund der rasant voranschreitenden technischen Entwicklung ist eine europaweit gültige Regelung, die Bewerber, Beschäftigte und ehemalige Mitarbeiter wirksam vor ausufernder Datenverarbeitung schützt und die gleichzeitig die Verarbeitungsmöglichkeiten von Arbeitgebern auf ein aus objektiver Sicht notwendiges Minimum beschränkt, mehr als wünschenswert. Einen derart umfassenden Schutz sah zwar auch die Entwurfsfassung der EU-Kommission vom 25. Januar 2012 zu einer Europäischen Datenschutz-Grundverordnung (EU-DS-GVO) nicht vor. Der im ursprünglichen Entwurfstext zu diesem Thema enthaltene Art. 82 zielte aber darauf, in allen EU-Staaten einschlägige Gesetze in den Grenzen der EU-DS-GVO zu schaffen.

Von diesem dem Beschäftigtendatenschutz zuträglichen Ansatz hat sich die Entwurfsfassung des EU-Parlaments vom 12. März 2014 grundlegend entfernt. Diese Feststellung folgt einerseits aus den zahlreichen Änderungen im Verordnungstext, die zu einer deutlichen Reduzierung des ursprünglich vorgesehenen Datenschutzstandards führen. Bezogen auf den Beschäftigtendatenschutz leitet sie sich andererseits aus zahlreichen datenschutzrechtlichen Erlaubnistatbeständen ab, die nunmehr in den neu in Art. 82 eingefügten Abs. 1a bis 1d enthalten sind. Hinter diesen Erlaubnistatbeständen, die die Erhebungs-, Verarbeitungs- und Nutzungsbefugnisse der Arbeitgeber bezogen auf die derzeit in Deutschland bestehende rechtliche Situation massiv ausweiten würden, könnte kein nationaler Gesetzgeber zurückbleiben. Adäquate wirksame Schutzmechanismen zugunsten der Beschäftigten fehlen hingegen im Entwurfstext. Ein Teil der Regelungen in Art. 82 Abs. 1a bis 1d ähneln denen, die der in Deutschland kontrovers diskutierte Entwurf der CDU/FDP-Bundesregierung zu einem Beschäftigtendatenschutzgesetz enthielt.

Der Entwurf des EU-Parlaments zu Art. 82 EU-DS-GVO würde im Ergebnis zu einer „Beschäftigtendatenverarbeitungs-Erlaubnisverordnung“ führen:

- Durch den Textvorschlag zu Art. 82 Abs. 1b würde beispielsweise die Verarbeitung von Beschäftigtendaten auf Grundlage einer freiwilligen Einwilligung möglich, ohne dass Beschäftigte zugleich wirksam davor geschützt werden, bezüglich der Abgabe einer Einwilligung unter Druck gesetzt zu werden.

- Die Regelung in Art. 82 Abs. 1c Buchstabe a) lässt für den Fall, dass zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass im Beschäftigungsverhältnis eine Straftat oder eine andere schwerwiegende Pflichtverletzung begangen wurde, auch heimliche Verarbeitungen von Beschäftigtendaten zu. Einschlägig für schwerwiegende Pflichtverletzung wären nach deutschem Recht alle Sachverhalte, die eine außerordentliche Kündigung gemäß § 626 BGB legitimieren. Die Schwelle hierfür ist nach der Rechtsprechung nicht hoch.

- Durch die Regelung in Art. 82 Abs. 1c Buchstabe b) wird die offene Videoüberwachung für alle Betriebsteile legitimiert. Ausgenommen bleiben würden nur Räume bleiben, die der „privaten Lebensgestaltung“ der Arbeitnehmer dienen.

- Durch die Regelung in Art. 82 Abs. 1c Buchstabe c) würden ärztliche Untersuchungen pauschal zugelassen. Lediglich Datenerhebungen zum Zwecke von gentechnischen Tests und Analysen sollen grundsätzlich untersagt werden.

- Für den Fall, dass die private Nutzung von betrieblichen Kommunikationsdiensten erlaubt ist, räumt die nicht abschließende Aufzählung in Art. 82 Abs. 1c Buchstabe d) Arbeitgebern beispielsweise das Recht ein, anfallende Verkehrsdaten zur „Gewährleistung der Datensicherheit“ zu verarbeiten. Dies würde beispielsweise eine Auswertung der Verkehrsdaten durch „Data Leak Prevention-Systeme“ zu präventiven Zwecken beinhalten.

- Die Verarbeitung von Beschäftigtendaten müsste sich nach Art. 82 Abs. 1d nicht mehr auf das jeweilige Unternehmen beschränken. Der Verordnungsvorschlag begründet vielmehr ein Konzernprivileg für die Datenverarbeitung, das es unter Beachtung der in Kapitel V des Entwurfs zu findenden Vorgaben möglich machen würde, Beschäftigtendaten ggf. auch in Drittländern zu verarbeiten. Damit würde es internationalen Konzern möglich, Überprüfungen von Verkehrsdaten zu Zwecken der Datensicherheit irgendwo auf der Welt und damit außerhalb der Reichweite von Kontroll- und Mitbestimmungsrechten der Betriebs- und Personalräte durchzuführen.

- Art. 82 Abs. 1 Satz 1 sieht ausdrücklich vor, dass in den Mitgliedsstaaten durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Daten im Beschäftigungsverhältnis vereinbart werden können. Käme es zur Umsetzung dieser Regelung in das nationale Recht, könnten Betriebs- und Personalräte unter Druck gesetzt werden, einer Reduzierung von Datenschutzstandards zuzustimmen, etwa zu Zwecken der Beschäftigungssicherung.

- Aus Sicht von Beschäftigten positiv ist hingegen die Regelung in Art. 82 Abs. 1c Buchstabe e) des Parlaments-Entwurfs zu bewerten, durch die u.a. die Erstellung „schwarzer Listen“ zur Gewerkschaftszugehörigkeit verboten würde. Damit endet aber die Aufzählung von Regelungsbestandteilen schon, die aus der Sicht von Beschäftigten positiv zu bewerten sind.

Der Rat der EU hat am 15. Juni 2015 die vom EU-Parlament in Art. 82 eingefügten Abs. 1a bis 1d nicht in seinen Entwurfstext übernommen. Allerdings verzichtet er mit seiner geänderten Formulierung zu Art. 82 Abs. 1 Satz 1 nunmehr vollständig darauf, dass nationale Regelungen zum Beschäftigtendatenschutz „in den Grenzen dieser Verordnung“ (Vorschlag der EU-Kommission zu Abs. 1 Satz 1) oder „im Einklang mit den Regelungen“ der EU-DS-GVO (Vorschlag des EU-Parlaments zu Abs. 1 Satz 1) stehen müssen. Stattdessen sieht der Entwurf des Rats zu Art. 82 Abs. 1 Satz 1 nunmehr vor, dass die Mitglieds-

staaten „durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften“ zum Beschäftigtendatenschutz vorsehen können. Damit eröffnet auch der Entwurf des Rats zur EU-DS-GVO den Weg, Datenschutz per Betriebsvereinbarung oder Tarifvertrag zu regeln, was auch Verschlechterungen gegenüber der gesetzlichen Situation per Betriebsvereinbarung oder Tarifvertrag beinhalten kann.

Bedenklich an der Textfassung des Rats sind weitere Details wie etwa der Hinweis, dass die Datenverarbeitung auch zu Zwecken der Erfüllung „gesetzlicher (…) Pflichten des Managements“ erfolgen kann. Dies würde der Forderung von Arbeitgebern mehr Gewicht verleihen, die schon heute die Intensivierung von Datenverarbeitung aus Compliance-Gründen fordern, um das eigene Management vor Regressforderungen zu schützen.

Fazit

Der vom EU-Parlament vorgelegten Entwurfsfassung zu Art. 82 EU-DS-GVO geht es offenkundig nicht vorrangig um den Beschäftigtendatenschutz, sondern vielmehr um massive Erleichterungen für Arbeitgeber. Die Umsetzung dieser Textfassung in europäisches Recht würde aus deutscher Sicht zu einer deutlichen Schwächung des Schutzes der Persönlichkeitsrechte von Beschäftigten führen. Auf dieser Grundlage wären etwas umfassende präventive Massenscreenings, die in der Vergangenheit bei großen Datenschutzskandalen zum Rücktritt von Vorstandsvorsitzenden geführt haben, zukünftig datenschutzrechtlich nicht ausgeschlossen. Eine EU-Verordnung in dieser Form wäre letztlich kein Mittel zum Beschäftigtendatenschutz, sondern eine „Beschäftigtendatenverarbeitungs-Erlaubnisverordnung“.

Kritisch ist auch die Entwurfsfassung des Rats vom 15. Juli 2015 zu sehen. Dies folgt insbesondere daraus, dass Verschlechterungen der datenschutzrechtlichen Situation durch Kollektivvereinbarungen nicht etwa ausgeschlossen werden, sondern ausdrücklich zugelassen.

Im Ergebnis bedeutet dies nicht, dass der ursprüngliche Vorschlag der EU-Kommission den Beschäftigtendatenschutz optimal schützen würde. Die EU-DS-GVO vom 25. Januar 2012 überließ aber zumindest die inhaltliche Ausgestaltung einschlägiger Gesetze vollständig den einzelnen EU-Staaten. Dies beinhaltet die Möglichkeit, gesetzliche Besonderheiten und Vorgaben der Rechtsprechung bei der Schaffung spezifischer Beschäftigtendatenschutzgesetze zu berücksichtigen. Problematisch ist aus heutiger Sicht allerdings, dass die „Grenzen dieser Verordnung“ durch die Umsetzung zahlreicher Änderungsvorschläge inzwischen vielfach nicht mehr gegeben sind. Ein wirksamer Beschäftigtendatenschutz ist damit auch auf Grundlage des modifizierten Entwurfs der EU-Kommission in weite Ferne gerückt.

Die Deutsche Vereinigung für Datenschutz e.V. dankt den elf beteiligten Organisationen und Einzelpersonen, die ihre roten Linien zur EU-DSGVO in kurzen Beiträgen dargestellt haben.
Es fällt auf, dass bestimmte rote Linien immer wieder genannt werden, hier ist besonders die Zweckbindung, die ausdrückliche Einwilligung sowie die Pflicht einen Datenschutzbeauftragten zu bestellen gefolgt von Datensparsamkeit und Profilbildung zu nennen. Einige Beiträge haben sich nur Einzelthemen herausgegriffen und diese ausführlicher dargestellt.

Bei allen genannten roten Linien muss bei den Trilog-Verhandlungen sichergestellt werden, dass diese nicht überschritten werden.

Wir hoffen, dass die Entscheidungsträger aus EU-Kommission, EU-Parlament und EU-Rat bei den Trilog-Verhandlungen diese Beiträge zur Kenntnis nehmen, sich den Argumentationen anschließen können und entsprechend handeln.

Die folgenden Organisationen und Einzelpersonen haben sich mit Beiträgen beteiligt (soweit nicht bei den Artikeln ausdrücklich angegeben liegt die Autorenschaft bei den jeweiligen Organisationen insgesamt):
Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit – www.bfdi.bund.de, Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. – www.bvdnet.de, Digitalcourage e.V. – www.digitalcourage.de, Digitale Gesellschaft e. V. – www.digitalegesellschaft.de, Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. – www.fiff.de, Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. – www.gdd.de, Konferenz der Datenschutzbeauftragten des Bundes und der Länder – www.datenschutz.de/dsb-konferenz, Professor Douwe Korff – www.korff.co.uk/douwe, Peter Schaar – www.eaid-berlin.de, Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. (vzbv) – www.vzbv.de, Prof. Dr. Peter Wedde – www.da-consulting.de

Campact hat bei der Vorbereitung und bei dem Versand dieses Sonderhefts unterstützt.

Im Anschluss an den folgenden Campact-Appell finden Sie thematisch passend die aktuelle Pressemitteilung des Europäischen Datenschutzbeauftragten zur EU-DSGVO und die Resolution zur EU-DSGVO des evangelischen Kirchentages 2015.

148.466 Menschen fordern:

GEGEN DIE DATENFALLEN DER KONZERNE:

STARKER EUROPÄISCHER DATENSCHUTZ JETZT!

V.i.S.d.P.: Katharina Nocun, Artilleriestraße 6, 27283 Verden

Unser Grundrecht auf informationelle Selbstbestimmung und Privatsphäre gegenüber Regierungen und Konzernen lässt sich nur europaweit durchsetzen. Deswegen unterstützen wir die von der EU-Kommission vorgelegte Datenschutz-Verordnung.

Personenbezogene Daten dürfen nicht ohne Wissen und ausdrückliche Zustimmung der Betroffenen gespeichert, ausgewertet und weiterverkauft werden. Es muss einen Anspruch auf Löschung und Mitnahme der eigenen Daten – etwa aus sozialen Netzwerken – geben.

Wir fordern Bundesregierung und Europaabgeordnete auf, keiner Verordnung zuzustimmen, die hinter das deutsche Datenschutzrecht zurückfällt.

Nutzen Sie die Chance, ein hohes Schutzniveau in der ganzen EU zu schaffen!

UNTERZEICHNEN SIE UNSEREN APPELL: WWW.CAMPACT.DE/EU-DATENSCHUTZ













Entwurf: zitrusblau.de



PRESSEMITTEILUNG

EDPS/2015/06

Brüssel, Montag, 27. Juli 2015

Ein neues Kapitel für den Datenschutz

Als der Europäische Datenschutzbeauftragte heute seine **Empfehlungen** an die Mitgesetzgeber der EU übermittelte, die den endgültigen Text der **Datenschutz-Grundverordnung** aushandeln, stellte er auch eine Handy-**App** vor, mit der sich die aktuellen Texte der Kommission, des Parlaments und des Rates einfacher auf Tablets und Smartphones **vergleichen** lassen.

Giovanni Buttarelli, der Europäische Datenschutzbeauftragte (EDSB), meinte dazu: "*Privatsphäre und Datenschutz sind für die Menschen wichtiger als je zuvor. Zum ersten Mal in einer Generation hat die EU die Möglichkeit, die Vorschriften darüber, wie mit personenbezogenen Daten umgegangen wird, zu* ***modernisieren****, zu* ***harmonisieren*** *und zu* ***vereinfachen.*** *Diese Vorschriften müssen für die* ***nächste Generation*** *von Technologien anwendbar sein. Da es zu meinem Aufgabenbereich gehört,* ***proaktiv*** *und* ***konstruktiv*** *vorzugehen, sollen meine Empfehlungen die Mitgesetzgeber dabei unterstützen,* ***ein besseres Ergebnis*** *für* ***natürliche Personen*** *zu erzielen, die Garantien in der Praxis wirksamer zu gestalten und sie in die Lage zu versetzen,* ***Nutzen*** *aus den technologischen Neuerungen zu* ***ziehen.*** *Die Datenschutz-Grundverordnung ist zwar nicht die Reform, von der ich geträumt habe, doch ich unterstütze die Organe auf der letzten Meile mit Nachdruck, damit sie das bestmögliche Ergebnis erzielen; Verbesserungen sind nach wie vor möglich.*"

Die Empfehlungen des EDSB sind zwangsläufig in Einklang mit den **Vorgaben** der Verhandlungen formuliert, an denen die drei wichtigsten EU-Organe (Trilog) beteiligt sind, und halten sich daher strikt an deren Texte. Der EDSB ist allerdings sehr **innovativ** vorgegangen, denn er hat sich für pragmatische Lösungen eingesetzt, die auf einer über zehnjährigen Erfahrung im Bereich der Aufsicht, Politikempfehlung und weltweiten Partnerschaft aufbauen. Die Empfehlungen des EDSB wurden im Interesse von Transparenz und Rechenschaftspflicht veröffentlicht.

Die vorgeschlagenen neuen Vorschriften werden sich potenziell auf alle natürlichen Personen in der EU, auf alle Organisationen in der EU, die personenbezogene Daten verarbeiten, sowie auf Organisationen außerhalb der EU, die personenbezogene Daten von natürlichen Personen in der EU verarbeiten, auswirken. Die übrige Welt blickt daher gespannt auf uns. Die Qualität des neuen EU-Datenschutzrechts, sein zukunftsorientierter Ansatz und die Art und Weise, wie dieser mit den weltweiten Rechtssystemen und rechtlichen Entwicklungen zusammenwirkt, sind von überragender Bedeutung. Europa kann international **mit gutem Beispiel vorangehen.**

Der EDSB ist der Auffassung, dass die EU den Datenschutz neu ordnen muss: sie braucht einen „neuen Deal“ und sollte ein neues Kapitel aufschlagen, das weniger auf übermäßige Formalitäten oder ein zu reglementierendes Vorgehen ausgerichtet ist, sondern mehr auf **dynamisch gestaltete Garantien** setzt, damit **natürliche Personen** die Kontrolle über die sie betreffenden Daten in der Welt der „Big Data“, in der wir leben, haben. Beim Umgang mit dem rasanten Technologiewandel sollten Leitlinien und vorbildliche Verfahren von gestärkten und wirklich unabhängigen Datenschutzbehörden Hilfestellung bieten.

Der EDSB hält die Mitgesetzgeber dazu an, bei dem endgültig vereinbarten Text an der **Würde des Einzelnen** und der **Menschenwürde** festzuhalten und diese in den **Vordergrund** zu rücken: natürliche Personen müssen geschützt werden, und zwar nicht nur deshalb, weil sie Benutzer, Abonnenten oder Verbraucher sind. Wir sollten es nicht zulassen, dass uns die Technologie unsere **Rechte** und **Freiheiten vorschreibt** oder **einschränkt.**

Wojciech Wiewiórowski, Stellvertretender Beauftragter, erklärte: "***Privatsphäre** und **Datenschutz** sind keine Hindernisse für wirtschaftliches Wachstum und internationalen Handel, sondern **fördern** diese. **Vertrauen** ist die notwendige Voraussetzung für innovative Produkte und Dienstleistungen, die auf die Verarbeitung personenbezogener Daten angewiesen sind. Das Bemühen der EU, den **digitalen Binnenmarkt** auszubauen, wird nur dann von Erfolg gekrönt sein, wenn die Interessen von natürlichen Personen geschützt werden. Ein „neuer Deal“ für die Bürgerrechte kann verantwortungsbewusste Unternehmen und staatliche Behörden wachrütteln*."

Hintergrundinformationen

Privatsphäre und Datenschutz sind Grundrechte in der EU. Datenschutz ist ein Grundrecht, das durch europäisches Recht geschützt und in Artikel 8 der Charta der Grundrechte der Europäischen Union verankert ist.

Konkret sind die Datenschutzbestimmungen für die EU-Organe - sowie die Pflichten des Europäischen Datenschutzbeauftragten (EDSB) - in der **Verordnung (EG) Nr. 45/2001** geregelt. Der Europäische Datenschutzbeauftragte (EDSB) ist eine relativ neue, aber zunehmend einflussreiche unabhängige Aufsichtsbehörde, die die Verarbeitung personenbezogener Daten durch die Einrichtungen und Organe der EU überwacht, in Bezug auf politische Maßnahmen und Rechtsvorschriften, die sich auf die Privatsphäre auswirken, beratend tätig ist und mit vergleichbaren Behörden zusammenarbeitet, um einen kohärenten Datenschutz sicherzustellen.

Giovanni Buttarelli (EDSB) und **Wojciech Wiewiórowski** (Stellvertretender EDSB) sind Mitglieder dieser Behörde und wurden durch eine gemeinsame Entscheidung des Europäischen Parlaments und des Rates ernannt. Sie traten ihre fünfjährige Amtszeit am 4. Dezember 2014 an.

Strategie des EDSB für den Zeitraum 2015-2019: In dem am 2. März 2015 vorgelegten Plan für den Zeitraum 2015-2019 werden die wichtigsten Herausforderungen im Bereich Datenschutz und Schutz der Privatsphäre für die kommenden Jahre sowie die drei strategischen Ziele und die zehn Begleitmaßnahmen des EDSB, um diesen Herausforderungen zu begegnen, zusammengefasst. Die Ziele lauten: 1.) Datenschutz wird digital 2.) Aufbau globaler Partnerschaften und 3.) Ein neues Kapitel für den Datenschutz in der EU.

Personenbezogene Daten bzw. Informationen: Alle Informationen, die sich auf eine bestimmte oder bestimmbare (lebende) natürliche Person beziehen. Beispiele hierfür sind u. a. Namen, Geburtsdaten, Fotos, Videoaufnahmen, E-Mail-Adressen und Telefonnummern. Weitere Angaben wie z. B. IP-Adressen und Inhalte von Mitteilungen, die sich auf Endnutzer von Kommunikationsdiensten beziehen oder von ihnen zur Verfügung gestellt werden, gelten ebenfalls als personenbezogene Daten.

Privatsphäre: Das Recht einer natürlichen Person, alleine gelassen zu werden und die Kontrolle über die Informationen über sich selbst auszuüben. Das Recht auf Privatsphäre und auf ein Privatleben ist in der Allgemeinen Erklärung der Menschenrechte (Artikel 12), der Europäischen Menschenrechtskonvention (Artikel 8) und der Europäischen Charta der Grundrechte (Artikel 7) verankert. Die Charta umfasst auch ein ausdrückliches Recht auf Schutz personenbezogener Daten (Artikel 8).

Verarbeitung personenbezogener Daten: Im Sinne von Artikel 2 Buchstabe b der Verordnung (EG) Nr. 45/2001 bezeichnet der Ausdruck „Verarbeitung personenbezogener Daten“ „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Wiederauffinden, das Abfragen, die Nutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten.“ Siehe hierzu auch das Glossar auf der EDSB-Website.

Große Datenmengen (Big Data): Gigantische digitale Datensätze im Besitz von Unternehmen, Regierungen und anderen großen Organisationen, die anschließend mittels Computeralgorithmen intensiv analysiert werden. Siehe hierzu auch die Stellungnahme 03/2013 der Artikel 29-Datenschutzgruppe zur Zweckbindung, S. 35.

Bei der Eurobarometer-Umfrage zum Datenschutz vom Juni 2015 wurde festgestellt, dass Datenschutz, insbesondere die Verarbeitung personenbezogener Daten in der digitalen Welt, für natürliche Personen in der EU nach wie vor ein wichtiges Anliegen ist.

EU-Datenschutzreformpaket: Am 25. Januar 2012 nahm die Europäische Kommission ihren Legislativvorschlag für die Datenschutz-Grundverordnung an, die direkt in allen EU-Mitgliedstaaten anwendbar ist. Der Standpunkt des Europäischen Parlaments wurde am 12. März 2014 in erster Lesung und der Standpunkt des Rates am 15. Juni 2015 angenommen. Das Europäische Parlament, der Rat der Europäischen Union und die Europäische Kommission befassen sich jetzt bei den Sitzungen des Trilogs mit der endgültigen Formulierung der Verordnung. Weitere Informationen über die Reform sind in dem speziell zu diesem Thema eingerichteten Bereich auf der Website des EDSB zu finden.

EU-Datenschutz ist eine kostenlose App des EDSB für mobile Endgeräte. Damit können alle Interessierten die neuesten Textvorschläge für die anstehende Datenschutz-Grundverordnung der Europäischen Kommission, des Europäischen Parlaments und des Rates der Europäischen Union vergleichen. Die App enthält auch die neuesten Empfehlungen des EDSB an die Mitgesetzgeber. Alle Texte können in einer beliebigen Kombination geladen und dann Seite für Seite verglichen werden (auf Smartphones aufgrund der begrenzten Bildschirmgröße maximal zwei Texte gleichzeitig).

Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Aufsichtsbehörde, deren Aufgabe es ist, dafür zu sorgen, dass der Schutz personenbezogener Daten und der Privatsphäre gewährleistet ist und bewährte Verfahren in den Organen und Einrichtungen der EU gefördert werden. Er erfüllt diese Aufgabe, indem er

- die Verarbeitung personenbezogener Daten durch die EU-Verwaltung überwacht,
- in Bezug auf politische Maßnahmen und Rechtsvorschriften, die sich auf den Schutz der Privatsphäre auswirken, beratend tätig ist und
- mit vergleichbaren Behörden zusammenarbeitet, um einen einheitlichen Datenschutz sicherzustellen.

Die Empfehlungen des EDSB sind auf der Website des EDSB abrufbar. Weitere Informationen:
press@edps.europa.eu

EDSB - Der europäische Hüter des Datenschutzes
www.edps.europa.eu

 Folgen Sie uns auf Twitter: @EU_EDPS

Diese Pressemitteilung als PDF sowie die EU-Data-Protection-App, die englische Version der Pressemitteilung und auch die Themenseite des EDPS finden Sie unter den folgenden Links:

Pressemitteilung des EDPS zur Reform der EU-Datenschutzgrundverordnung vom 27.07.2015 (deutsch):
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2015/EDPS-2015-06-EDPS_GDPR_DE.pdf

Pressemitteilung des EDPS zur Reform der EU-Datenschutzgrundverordnung vom 27.07.2015 (englisch):
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2015/EDPS-2015-06-EDPS_GDPR_EN.pdf

Themenseite zur EU-Datenschutzgrundverordnung des EDPS (englisch):
https://secure.edps.europa.eu/EDPSWEB/edps/Consultation/Reform_package

Empfehlungen des EDPS zur EU-Datenschutzgrundverordnung (englisch):
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_EN.pdf

Tabellarische Darstellung der Empfehlungen des EDPS zur EU-Datenschutzgrundverordnung (englisch):
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_Annex_EN.pdf

Die EU-Data-Protection-App im Apple-Store:
https://itunes.apple.com/us/app/eu-data-protection/id1014393191?ls=1&mt=8

Die EU-Data-Protection-App im Google Store:
https://play.google.com/store/apps/details?id=eu.europa.edps.dataprotection

Evangelischer Kirchentag 3.-7. Juni 2015 in Stuttgart

Rettet unsere Grundrechte – für einen starken Datenschutz in Europa!

Antragsteller/in:
Rena Tangens, Digitalcourage e.V., Marktstraße 18, 33602 Bielefeld

Adressat:
Thomas de Maizière, Bundesinnenminister

Text:
Appell an den Bundesinnenminister: Bekennen Sie sich eindeutig zum Datenschutz Ihrer Bürgerinnen und Bürger, statt sie den internationalen Datenmärkten auszuliefern!

Begründung:
Globale Big-Data-Konzerne sehen unsere persönlichen Daten als das neue Erdöl und sind entsprechend rücksichtslos dabei, sie auszubeuten. Die datensammelnde Wirtschaft will möglichst ungehindert Zugriff auf all unsere Daten haben.

Noch im Juni will der EU-Ministerrat seine Fassung der Datenschutzverordnung beschließen. Die EU würde damit grundlegende Prinzipien über Bord werfen, die uns schützen. Das betrifft uns alle – denn wenn die EU-Datenschutzverordnung in Brüssel beschlossen wird, gilt sie unmittelbar und deutsches Datenschutzrecht wird hinfällig.

Es ist Aufgabe der Politik, der Datengier Schranken zu setzen und die Persönlichkeitsrechte der Bürgerinnen und Bürger per Gesetz wirksam zu schützen. Leider tut das hierfür verantwortliche Innenministerium bei den Verhandlungen im EU-Ministerrat das Gegenteil. Statt die Grundrechte der Bürgerinnen und Bürger zu schützen, hat es offen Ohren für die Lobbyisten der Daten-Dealer.

Für uns ist unsere Menschenwürde unverzichtbar. Wir wollen nicht auf Zahlen reduziert werden. Wir wollen auch morgen unsere Entscheidungsfreiheit nicht an Algorithmen von Konzernen abgeben.



Befürworter der Grundrechte bei dem Kirchentag.
Bildquelle: https://www.kirchentag.de/programm/resolutionen.html

Jetzt im Juni ist die allerletzte Chance, im zukünftigen europäischen Recht unsere Werte zu verteidigen. Wenn das Datenschutzrecht schwach ist, dann verlieren die Menschen in der digitalen Welt ihre Freiheit.

Wir appellieren an den Bundesinnenminister:

Bekennen Sie sich eindeutig zum Datenschutz Ihrer Bürgerinnen und Bürger, statt sie den internationalen Datenmärkten auszuliefern!

Setzen Sie sich im EU-Ministerrat entschieden für folgende Punkte ein:

1. Bürgerinnen und Bürger sollen das Recht auf einen datenschutzfreundlichen Service bekommen. (privacy-friendly-service)
2. Leistungen dürfen nicht von der Preisgabe unnötiger Daten abhängig gemacht werden. Das heißt, eine Taschenlampen-App muss auch funktionieren, wenn wir keinen Zugriff auf unser Adressbuch geben. (Datensparsamkeit und Kopplungsverbot)
3. Daten dürfen nur für die Zwecke verwendet werden, für die sie erhoben wurden. (Zweckbindung)
4. Bürgerinnen und Bürger müssen der Verarbeitung ihrer Daten ausdrücklich zustimmen. Es reicht nicht, wenn Firmen behaupten, sie hätten ein “berechtigtes Interesse”. Nur die informierte Zustimmung sichert unser Recht auf informationelle Selbstbestimmung. (explizite Einwilligung)
5. Forschung darf keine Hintertür für Firmen werden, persönliche Daten beliebig und ohne Zustimmung der Betroffenen zu nutzen. Dies gilt insbesondere für Daten, die Rückschlüsse auf die Gesundheit zulassen.

Jörg Pohle

Zweckbindung revisited

Einleitung

Das datenschutzrechtliche Prinzip der Zweckbindung steht vermehrt unter Beschuss. So hat etwa der ITK-Verband BITKOM gerade erst öffentlich die Abschaffung der Zweckbindung gefordert.[1] Damit steht der Verband keineswegs allein. Im Rahmen einer schriftlichen Anhörung hatte das BMI erst Ende 2014 gemeinsam mit dem BMWi und dem BMJV unter anderem sehr zielgerichtet gefragt, »welche Bedeutung das Erfordernis der Kompatibilität des geänderten Zwecks einer Datenverarbeitung mit dem Erhebungszweck für bestehende und künftige Geschäftsmodelle sowie für die Rechte und Interessen der Betroffenen habe« und »welche Folgen es für diese Geschäftsmodelle sowie für die Betroffenen hätte, wenn eine mit dem Erhebungszweck unvereinbare Zweckänderung aufgrund überwiegender berechtigter Interessen des Datenverarbeiters (Art. 6 Abs. 1 lit. f DS-GVO-E) ausgeschlossen wäre.« Von wenigen Ausnahmen abgesehen, sind die eingegangenen Stellungnahmen bisher nicht veröffentlicht worden – die Ergebnisse der Anhörung sind jedoch umso sichtbarer: Die Innen- und Justizminister der EU-Mitgliedsländer haben im EU-Rat beschlossen, das Zweckbindungsprinzip auszuhebeln.[2]

Vor diesem Hintergrund soll das Zweckbindungsprinzip als Artefakt[3] einer spezifischen Operationalisierung des Datenschutzes im Recht beleuchtet und eingeordnet werden. Dabei sollen nicht nur schlaglichtartig die Genese dieses Rechtsgrundsatzes und seine historischen Begründungen erörtert, sondern auch einer der ihm zunehmend entgegen gehaltenen zentralen Kritikpunkte widerlegt werden – die vermeintliche Veralterung des Zweckbindungsgrundsatzes aufgrund neuerer technischer Entwicklungen, wie sie etwa unter dem Schlagwort »Big Data« zusammengefasst werden.

Die historischen Konstruktionen des Zweckbindungsgrundsatzes

Informierte Einwilligung und Zweckbindung

Der Grundsatz der Zweckbindung hat die moderne information privacy- und Datenschutzdebatte schon seit ihrem Beginn in den 1960er Jahren begleitet.

Die »Special Committee on Science and Law« der New Yorker Anwaltskammer formulierte im Rahmen einer wissenschaftlichen Untersuchung die Anforderungen, denen eine verantwortbare Verhaltensforschung am Menschen zu genügen habe. Der Kommissionsvorsitzende Oscar M. Ruebhausen und der Präsident der Russell Sage Foundation Orville G. Brim, Jr. veröffentlichten die Untersuchungsergebnisse, die sich dem Spannungsverhältnis zwischen wissenschaftlicher Forschung und der »private personality« widmen, Ende 1965 in der Columbia Law Review.[4]

Als eine der wesentlichen Anforderungen identifizieren sie unter Verweis auf die Ergebnisse des Nürnberger Ärzteprozesses die Notwendigkeit eines »fully informed consent, freely given, of the individual person being examined«.[5] Neben einer Diskussion über die notwendigen Eigenschaften der Einwilligung – explizit oder implizit, informiert, freiwillig – stellen die Autoren fest, dass eine Einwilligung immer nur kontext- und zweckbezogen sein könne mit der Folge einer Kontext- und Zweckbindung für den Umgang mit den erhobenen Informationen:

»Moreover, consent to the revelation of private personality for one purpose, or under one set of circumstances, is not license to publish or use the information so obtained for different purposes or under different conditions.«[6]

Die Einwilligung wirke dabei nicht nur hinsichtlich der Kontext- und Zweckdimension einschränkend, sondern auch »to the methods to be used, the risks to be taken, the degree of information the subject wishes to give or receive, the type of data to be obtained, or the uses to which it may be put.«[7]

Einer sehr ähnlichen Begründung bedient sich fünf Jahre später das Bundesverfassungsgericht im Ehescheidungsakten-Beschluss vom 15. Januar 1970.[8] Auch der damalige Bundesminister der Justiz hatte in seiner Stellungnahme an das Gericht auf den »begrenzten Kundgebungszweck« verwiesen, mit dem »Details aus der ehelichen Intimsphäre« in einem Ehescheidungsverfahren vorgetragen würden, nur darauf beziehe sich der »Wille der Beteiligten«. Diese Beschränkung werde »von der Rechtsordnung durch die Bestimmungen über die Nichtöffentlichkeit der Verhandlung und die Amtsverschwiegenheit entsprechend gesichert.«[9] Das Bundesverfassungsgericht folgt in seinem Beschluss dieser Argumentation und stellt fest, dass »die Offenlegung in bezug auf den Adressatenkreis – das Gericht und die Verfahrensbeteiligten – und in bezug auf den verfolgten Zweck – Herbeiführung der Gerichtsentscheidung – inhaltlich begrenzt« sei. Eine Übersendung der Akten für andere Zwecke sei somit ein Eingriff in das Persönlichkeitsrecht der Ehegatten und ohne ihr Einverständnis nur dann zulässig, wenn sie nach dem Verhältnismäßigkeitsprinzip gerechtfertigt sei.[10] Eine solche Rechtfertigung vermochte das Gericht jedenfalls in Bezug auf die disziplinarische Verfolgung von Dienstvergehen nicht zu erkennen.

Das damit verfolgte Ziel ist offensichtlich: Die Einwilligung soll bedeutungsvoll gemacht werden, indem mit der Zwecksetzung – und der darauf aufbauenden Zweckbindung – eine der wesentlichen Eigenschaften von Information und Informationsverarbeitung der Entscheidungsprärogative der Betroffenen unterworfen wird. Die Zweckbindung ist insoweit ein Artefakt der Ent-

scheidung, die Informationserhebung, -verarbeitung und -nutzung von der Einwilligung der Betroffenen abhängig zu machen.

Phasenorientierung und Zweckbindung

In ihrem 1971 für das Bundesministerium des Innern erstellten und 1972 veröffentlichten Gutachten »Grundfragen des Datenschutzes«,[11] dessen dort entwickelte Regelungsarchitektur bis heute das Datenschutzrecht prägt, nicht nur das bundesdeutsche,[12] beziehen sich Wilhelm Steinmüller et al. explizit auf diese Entscheidung des Bundesverfassungsgerichts und die dort formulierte »Zweckentfremdungsregel«, d. h. das »Verbot, Individualinformationen, die für einen bestimmten Zweck ermittelt sind, einem anderen Zweck zuzuführen.«[13] Damit erweitern sie gleichzeitig den Geltungsbereich des Zweckbindungsgrundsatzes: Nicht nur auf Basis einer Einwilligung erhobene personenbezogene Informationen, sondern alle personenbezogenen Informationen dürften ausschließlich zu dem Zweck verarbeitet werden, zu dem sie erhoben wurden.[14]

Die Autoren knüpfen damit direkt an das von ihnen zugrunde gelegte Informationskonzept an[15] und lösen gleichzeitig elegant das Zeitproblem, das sie mit ihrer phasenorientierten Gestaltung des Datenschutzrechts geschaffen haben.

Dieser Operationalisierungsansatz knüpft an einen »tatsächlichen Prozeß [an]; er geht also von einer (zugleich gesellschaftlichen wie „technischen“) Realität aus.«[16] Dieser Prozess ist die Informationsverarbeitung, die »eine typische Struktur aufweist«: »eine regelmäßige Wiederkehr gleicher Zustände des Prozesses der [Informationsverarbeitung]«.[17] An diesen Prozess – den »Ort des Problems« – und seine einzelnen »Phasen« ließen sich dann rechtliche Anforderungen formulieren.[18] Die im Gutachten formulierten und später ins BDSG übernommenen Anforderungen betreffen jedoch jeweils nur eine Phase, nicht jedoch den Prozess insgesamt.[19] Eine der beiden phasenübergreifenden Konstanten, die den ganzen Prozess rechtlich klammern, ist der Zweck, der vor der Erhebung der Information festgelegt wird und an den die verantwortliche Stelle bis zur Informationslöschung gebunden ist. Die andere Konstante ist der Personenbezug: Solange er besteht, muss er gleich bleiben; seine Aufhebung bietet jedoch eine Möglichkeit zur »Flucht aus dem Datenschutzrecht«.[20]

Beide Konzepte – der Personenbezug von Informationen und die Zweckbindung – lassen sich damit deutlich als Artefakte der jeweils zugrunde liegenden Operationalisierungsentscheidungen identifizieren: Die Wahl des Informationskonzepts der Semiotik bietet mit der sigmatischen Informationsdimension eine rechtliche Anknüpfungsmöglichkeit für die bezeichnete Person und ermöglicht es – jedenfalls grundsätzlich –, zu jedem Zeitpunkt während des Informationsverarbeitungsprozesses rechtlich verbindlich festzustellen, wer Rechte gegenüber der verantwortlichen Stelle wahrnehmen darf und wem gegenüber die verantwortliche Stelle begründungs- und nachweispflichtig ist. Und wenn vor dem Hintergrund einer außerhalb des faktischen Herrschafts- und damit Eingriffsbereichs der Betroffenen individuelle Eingriffsrechte und -möglichkeiten geschaffen werden sollen, erfordert das gerade ein Konzept wie den Personenbezug.

Andererseits wird mit der Operationalisierung des Datenschutzes im Recht über die einzelnen Phasen des Informationsverarbeitungsprozesses ein Zeitproblem erzeugt: Die Dauer des Prozesses muss nicht a priori determiniert sein, auch müssen die einzelnen Phasen zeitlich nicht direkt aneinander anschließen. Weil darüber hinaus grundsätzlich alle Bestandteile des Prozesses variabel sind – technische Verfahren und Datenverarbeitungsmittel, die verarbeitende Stelle,[21] deren innere Organisation und die mit der Verarbeitung betrauten Personen u. v. m. –, existiert gerade keine natürliche Konstante als Prüfanker, von dem aus alle anderen Aspekte zu jedem Zeitpunkt während des Informationsverarbeitungsprozesses abgeleitet bzw. nachträglich überprüft werden können. Ein solcher Prüfanker muss demnach explizit konstruiert und in das Recht eingeschrieben werden. Der Personenbezug ist dabei kein für diesen Zweck geeigneter Prüfanker, denn anhand dessen lassen sich weder die eingesetzten Mittel prüfen noch Erhebungs- und Verwendungskontexte. Personenbezug stellt nur die Verbindung zu den subjektiven Rechten her, während die objektivrechtliche Dimension – die »zweite Säule des Datenschutzrechts«[22] – gerade mit dem Zweckbindungsprinzip adressiert wird.

Kontrollierbarkeit und Zweckbindung

Es ist Bernhard Hoffmanns Verdienst, die erste – und bislang einzige – umfassende Analyse der Rolle des Zweckbindungsgrundsatzes in der rechtlichen Operationalisierung, die der Datenschutz im bundesdeutschen Datenschutzrecht gefunden hat, vorgelegt zu haben.[23] In seiner Betrachtung beschränkt er sich allerdings deutlich auf die Erforderlichkeit des Zweckbindungsprinzips für die »Wahrung des ursprünglichen Erhebungskontexts«[24] und insbesondere für die Schaffung »wohlgeordnete[r], transparente[r] und kontrollierbare[r] Strukturen«.[25] Die Rolle des Zweckbindungsgrundsatzes für die Sicherstellung einer bedeutungsvollen Einwilligung der Betroffenen und die Lösung des Zeitproblems des prozeduralen Datenschutzrechtsansatzes bleiben demgegenüber überraschend ausgeblendet.

Einerseits sind Zwecke strukturbildend, sie definieren Bereiche und damit die Grenzen zwischen den Bereichen, die zur Informationsflusskontrolle genutzt werden können.[26] Andererseits dienen sie der Bestimmung der Menge der für die Zweckerreichung, also innerhalb der Bereiche, funktional äquivalenten Handlungsmöglichkeiten und Mittel.[27] Datenschutzrechtlich handelt es sich dabei um die Bestimmbarkeit der Geeignetheit. Die Setzung von Zwecken trennt dabei den Raum aller überhaupt möglichen Handlungen und Mittel sowie ihrer Wirkungen in erwünschte und unerwünschte.[28] Zugleich eröffnet die Zwecksetzung die Möglichkeit, die grundsätzlich erwünschten Handlungsalternativen und Mittel sinnvoll miteinander vergleichen zu können,[29] so etwa zur Unterscheidung zwischen erforderlichen und nicht erforderlichen Handlungen und Mitteln. Auf dieser Basis kann abschließend die Angemessenheit

der Handlungen und Mittel adressiert werden. Mit der Zweckbindung, der »Gewährleistung einer ausschließlich zweckbestimmten Verwendung«,[30] wird dann Kongruenz von Sollen und Sein sichergestellt.

Das Zweckbindungsprinzip ist demnach Mittel zur Erzeugung von Kontrollierbarkeit der Informationserhebung, -verarbeitung und -nutzung sowie der dabei verwendeten technischen wie nicht-technischen Mittel, indem es wohlgeordnete Organisationsstrukturen und Prozesse erzeugt, die zugleich transparent gemacht werden können – den Organisationen selbst, vor allem jedoch den Betroffenen und den Aufsichtsbehörden.

Zweckbindung ist nicht veraltet

Im Ergebnis stellt sich Zweckbindung nicht notwendigerweise als Teil einer Datenschutz- oder information privacy-Theorie dar, sondern in erster Linie als ein Artefakt spezifischer Operationalisierungen und Umsetzungen im Recht. Sie dient als konzeptionelle und operationale Klammer um den Prozess von Informationserhebung, -verarbeitung und Entscheidungsfindung, indem sie als Konstante in einem dynamischen Umfeld wirkt und damit einen festen Anker für die Prüfung sowohl der Handlungen wie der eingesetzten Mittel bietet. Zugleich stellt sie bei hoheitlichen Informationsverarbeitungsprozessen sicher, dass diese grundsätzlich auf die konkrete behördliche Aufgabe beschränkt und die Anforderungen der zur Erhebung ermächtigenden Rechtsgrundlage gewahrt bleibt.[31]

Zwecksetzung ist dabei entweder Fremd- oder Selbstbindung, Zweckbindung ist dessen überprüfbare Einhaltung. Während der öffentliche Bereich durch Fremdbindung in Form von Zweck- und Aufgabenzuweisung geprägt ist, handelt es sich im nicht-öffentlichen Bereich in der Regel um eine Selbstbindung, also im Grunde eine Ausprägung von Selbstregulierung, dafür jedoch mit Compliance-Garantie.

Darüber hinaus war Zweckbindung schon immer kontrafaktisch. Seit der Erfindung der Schrift vor fast 6.000 Jahren durch die Sumerer speichern alle Datenträger, die die Menschheit je erfunden hat, ausschließlich Zeichen. Moderne Datenverarbeitungssysteme wie Computer sind reine Syntaxverarbeitungsmaschinen – Kontext- und Zweckfreiheit sind oft explizite Technikgestaltungsziele;[32] Kontexte und Zwecke den Systemen (wieder) beizubringen ist alles andere als einfach.[33]

Diese Eigenschaft der Multifunktionalität moderner IT-Systeme ist in der Datenschutzdebatte schon lange bekannt.[34] Zweckbindung war gerade die bewusste normative, aber eben auch kontrafaktische Antwort des Rechts auf moderne, grundsätzlich zweckfrei mögliche Informationsverarbeitung.[35] Demnach können Big-Data- und andere Verfahren moderner Informationsverarbeitung dieses normative Instrument auch nicht »einfach veralten« lassen – im Gegenteil: Gerade seine Fähigkeit zur effektiven Beschränkung der Informationsmacht der Datenverarbeiter macht das Zweckbindungsprinzip bei privaten wie öffentlichen Datenverarbeitern und deren jeweiligen Lobbyisten derart unbeliebt.[36]

Die Zukunft der Zweckbindung

Der Datenschutz adressiert das Problem der gesellschaftlichen Machtverteilung und Machtkontrolle unter den Bedingungen der Industrialisierung der gesellschaftlichen Informationsverarbeitung – vergleichbar zum »Problem des Verfassungsstaates im politischen Bereich und […] der Kontrolle der Produktionsverhältnisse im wirtschaftlichen Bereich«[37] – mit seinen Folgen für Mensch und Gesellschaft, Gruppen und Institutionen.[38] Viele überkommene Operationalisierungen gelten grundsätzlich oder in ihrer Umsetzung im Recht jedoch inzwischen als nicht mehr zeitgemäß, etwa der exzessive Fokus des Rechts auf die individuelle Einwilligung,[39] oder werden zu Recht hinterfragt, etwa die Möglichkeit der Grenzziehung beim Personenbezug von Informationen.[40] Vorschläge für alternative Regelungsansätze existieren, etwa unter Verwendung von Schutzzielen,[41] die seit den 1980er Jahren in der IT-Sicherheit erfolgreich eingesetzt werden. Aber lässt sich damit auch das Zweckbindungsprinzip ersetzen?

Als Alternative zur Nutzung der personenbezogenen Information als Anknüpfungsobjekt des Datenschutzrechts ließe sich etwa – wenn die Anbindung an das Individuum und die Möglichkeit zur Festschreibung von Betroffenenrechte beibehalten werden soll – an das Konzept der personenbezogenen Entscheidung rechtlich anknüpfen. Personenbezogene Entscheidungen seien dabei alle sozial relevanten Entscheidungen über Menschen in vermachteten Verhältnissen. Dies würde vor allem das Problem adressieren, dass Organisationen keineswegs – wie es der derzeitige Datenschutzrechtsansatz unterstellt – Menschen nur auf der Basis von Informationen sortieren, kategorisieren, bewerten und über sie entscheiden, die personenbezogen im Sinne des Datenschutzrechts sind, sondern durchaus auch auf der Basis von Gruppen- oder statistischen Informationen.[42] Über den Anknüpfungspunkt der personenbezogenen Entscheidung wären dann alle Informationen, ob personenbezogen oder nicht, die zur Grundlage dieser Entscheidung gemacht worden sind oder gemacht werden sollen, rechtlich adressierbar.[43]

Doch auch der Fokus des Datenschutzrechts auf die Einwilligung der Betroffenen ist nicht alternativlos. Mit dem das Rechtsstaatsprinzip adaptierenden Prinzip des »Systemdatenschutzes« steht längst ein angemessener Ersatz zur Verfügung:

»Systemdatenschutz heißt dann die Menge der Rechtsregeln, die Vorgänge der Informationserhebung oder der Informationsverarbeitung unabhängig davon, ob im Einzelfall Interessen der Betroffenen berührt sind oder nicht, rechtlich so ordnen, daß die Gesamtheit der rechtlich geregelten Informationsvorgänge keine sozialschädlichen Folgen herbeiführen.«[44]

Im Grunde nichts Neues – mit dem BDSG sind schon immer auch nicht-öffentliche Stellen aus dem Rechtsstaatsprinzip folgenden Anforderungen unterworfen;[45] dieser Ansatz wird inzwischen wieder deutlich lauter vertreten.[46]

Selbst die Phasenorientierung als zentrales Element des derzeitigen Datenschutzrechts und Mittel zur Komplexitätsreduktion für eine Analyse für die von der Informationsverarbeitung ausgehenden Gefahren kann zur Dis-

position gestellt werden. Schon in der EG-Datenschutzrichtlinie 95/46/EG von 1995 war sie nur noch rudimentär vorhanden. Mit den Entwürfen für eine EU-Datenschutzgrundverordnung hat sie weiter an Boden verloren, und mit dem Inkrafttreten der Verordnung würde sie aus dem deutschen Datenschutzrecht wohl einfach verschwinden. Auch der derzeit meistdiskutierte alternative Regelungsansatz, der auf der Verwendung von Schutzzielen basiert,[47] kommt ohne eine Phasenorientierung aus.[48]

Allein für das Zweckbindungsprinzip scheint keine geeignete Alternative in Sicht. Zwar gibt es wie beschrieben Bestrebungen zu seiner Abschaffung, auch wurden schon Abschwächungsvorschläge unterbreitet,[49] ein Vorschlag für einen funktional äquivalenten Ersatz, mit dem die Wahl der Mittel und ihre Verwendung sowohl entschieden wie geprüft werden kann, wurde bislang jedoch nicht vorgelegt. Und gerade diese Eigenschaft ist es, die den zentralen Wert des Zweckbindungsgrundsatzes ausmacht: Die Geeignetheit des Zwecks, ob selbst- oder fremdgesetzt, als Konstante und fester Prüfanker die Kontrollierbarkeit zunehmend komplexer Informationsverarbeitungs- und Entscheidungsprozesse, der beteiligten Akteure, ihrer Handlungen und der eingesetzten Mittel – von Hard- und Software über Algorithmen und Heuristiken bis zu den verwendeten Informationen – herzustellen und zu wahren. Wenn zum Schutz der einzelnen Betroffenen und der Gesellschaft insgesamt vor der strukturell überlegenen Informationsmacht von Organisationen die Ausübung dieser Macht einer Kontrolle unterworfen werden soll, führt am Prinzip der Zweckbindung derzeit kein Weg vorbei.

1 BITKOM (2015). EU-Datenschutzverordnung muss Innovationen ermöglichen. Presseerklärung vom 24.06.2015. url: http://www.bitkom.org/de/presse/8477_82534.aspx.

2 Stefan Krempl und Andreas Wilkens (2015). „EU-Datenschutzreform: Zweckbindung und Datensparsamkeit ausgehebelt“. In: heise online. 15.06.2015. url: http://heise.de/-2690862.

3 Artefakt kann einerseits allgemein etwas Menschengemachtes bezeichnen, andererseits jedoch auch ein – oft störendes – Phänomen, das als Folge von etwas wie der Wahl der Messmethode in der Sozialforschung oder des verwendeten Algorithmus bei der verlustbehafteten Bildkompression auftritt. Hier sollen beide Lesarten zusammengeführt werden: Es wird gezeigt, dass das Zweckbindungsprinzip einerseits Folgeprodukt vorhergehender Operationalisierungsentscheidungen ist, andererseits jedoch explizit Menschenwerk. Ein Beispiel: In einem mehrstöckigen Gebäude sind notwendig Höhenunterschiede zu überwinden. Rampen, Leitern, Treppen oder Lifte sind dafür geeignete Mittel. Dass solche Mittel überhaupt erforderlich sind, ist eine Folge der vorhergehenden Entscheidung, ein mehrstöckiges Gebäude zu bauen. Das gewählte Mittel, etwa der Lift, ist damit ein Artefakt dieser Entscheidung. Und es bleibt auch dann ein Artefakt der Entscheidung, wenn bewiesen werden kann, dass es unter den grundsätzlich geeigneten Mitteln das beste ist.

4 Oscar M. Ruebhausen und Orville G. Brim Jr. (1965). „Privacy and Behavioral Research“. In: Columbia Law Review 65.7, S. 1184–1211.

5 Ruebhausen und Brim 1965, S. 1198.

6 Ruebhausen und Brim 1965, S. 1199.

7 Ruebhausen und Brim 1965, S. 1199.

8 BVerfGE 27, 344. Ehescheidungsakten.

9 BVerfGE 27, 344, 348.

10 BVerfGE 27, 344, 352.

11 Wilhelm Steinmüller u. a. (1971). Grundfragen des Datenschutzes. Gutachten im Auftrag des Bundesministeriums des Innern, BT-Drs. VI/3826, Anlage 1.

12 Vgl. Jörg Pohle (2014a). „Die immer noch aktuellen Grundfragen des Datenschutzes“. In: Wovon – für wen – wozu. Systemdenken wider die Diktatur der Daten. Wilhelm Steinmüller zum Gedächtnis. Hrsg. von Hansjürgen Garstka und Wolfgang Coy. Humboldt-Universität zu Berlin, Hermann von Helmholtz-Zentrum für Kulturtechnik. Berlin, S. 45–58.

13 Steinmüller u. a. 1971, S. 115.

14 Zweckbindung müsse selbst für Informationen gelten, die »um einer öffentlichen – vor allem auch politischen – Wirkung willen ganz bewußt in die Öffentlichkeit« getragen worden seien, so die Datenschutzkommission des Deutschen Juristentages (1974). Grundsätze für eine Regelung des Datenschutzes. Bericht der Datenschutzkommission des Deutschen Juristentages. München: C. H. Beck’sche Verlagsbuchhandlung, S. 27.

15 In ihrem von der Semiotik übernommenen vierdimensionalen Konzept – Syntax, Semantik, Pragmatik und Sigmatik – wird der Zweck gerade über die pragmatische Dimension rechtlich adressierbar, siehe Steinmüller u. a. 1971, S. 42 f.

16 Steinmüller u. a. 1971, S. 54.

17 Steinmüller u. a. 1971, S. 57.

18 Steinmüller u. a. 1971, S. 57.

19 Zu den Hintergründen und zur Kritik siehe Jörg Pohle (i.E.). „Transparenz und Berechenbarkeit vs. Autonomie- und Kontrollverlust: Die Industrialisierung der gesellschaftlichen Informationsverarbeitung und ihre Folgen“. In: Mediale Kontrolle unter Beobachtung.

20 Zum Scheitern der damit verbundenen Erwartung an den Durchbruch datenvermeidender Verfahren siehe Paul Ohm (2010). „Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization“. In: UCLA Law Review 57, S. 1701–1777.

21 Das gilt etwa beim Rückgriff auf Auftragsdatenverarbeiter.

22 Steinmüller u. a. 1971, S. 60.

23 Bernhard Hoffmann (1991). Zweckbindung als Kernpunkt eines prozeduralen Datenschutzansatzes. Baden-Baden: Nomos Verlagsgesellschaft.

24 Hoffmann 1991, S. 127. Das ist Helen Nissenbaums »contextual integrity« avant la lettre, siehe Helen Nissenbaum (2004). „Privacy as contextual integrity“. In: Washington Law Review 79, S. 101–139. Gerade die konzeptionelle Verwandtschaft zwischen den verschiedenen Theorien zu den individuellen und gesellschaftlichen Folgen moderner Informationsverarbeitung wird jedoch in der Forschung bislang weitgehend ignoriert.

25 Hoffmann 1991, S. 26.

26 Hoffmann 1991, S. 25.

27 Hoffmann 1991, S. 81, mit Verweis auf Niklas Luhmann (1964). Funktionen und Folgen formaler Organisation. Berlin: Duncker & Humblot, S. 109.

28 Hoffmann 1991, S. 46.

29 Hoffmann 1991, S. 50.

30 Hoffmann 1991, S. 21.

31 Vgl. BVerfG, Urteil vom 24.04.2013, Rn. 113.

32 Das gilt vor allem für die Hardware, siehe schon Claude E. Shannon (1948). „A Mathematical Theory of Communication“. In: The Bell System Technical Journal 27.3, S. 379–423, S. 379.

33 Vgl. Jörg Pohle (2014b). „Kausalitäten, Korrelationen und Datenschutzrecht“. In:

Fundationes I: Geschichte und Theorie des Datenschutzes. Hrsg. von Jörg Pohle und Andrea Knaut. Münster: Monsenstein und Vannerdat, S. 85–105, Rn. 42 ff.

34 Zusammenfassend Wilhelm Steinmüller (1993). Informationstechnologie und Gesellschaft: Einführung in die angewandte Informatik. Darmstadt: Wissenschaftliche Buchgesellschaft, S. 488 ff. 35 Vgl. Martin Kutscha (1999). „Datenschutz durch Zweckbindung – ein Auslaufmodell?" In: Zeitschrift für Rechtspolitik 4, S. 156–160. 36 Siehe den Vergleich Chris Hoofnagles zwischen dem Fair Credit Reporting Act von 1970 und heutigen Vorschlägen für die Regulierung von Big Data: Chris Jay Hoofnagle (2013). „How the Fair Credit Reporting Act Regulates Big Data". In: Future of Privacy Forum Workshop on Big Data and Privacy: Making Ends Meet. 37 Adalbert Podlech (1976). „Gesellschaftstheoretische Grundlage des Datenschutzes". In: Datenschutz und Datensicherung. Hrsg. von Rüdiger Dierstein, Herbert Fiedler und Arno Schulz. Köln: J. P. Bachem Verlag, S. 311–326, S. 313.

38 Vgl. Pohle i.E.

39 Vgl. Bert-Jaap Koops (2014). „The trouble with European data protection law". In: International Data Privacy Law 4.4, S. 250–261.

40 Vgl. Paul M. Schwartz und Daniel J. Solove (2011). „The PII Problem: Privacy and a New Concept of Personally Identifiable Information". In: NYUL Review 86, S. 1814–1894.

41 Vgl. Martin Rost und Katalin Storf (2013). „Zur Konditionierung von Technik und Recht mittels Schutzzielen". In: Informatik 2013 : Informatik angepasst an Mensch, Organisation und Umwelt. Hrsg. von Matthias Horbach. Bd. 220. Lecture Notes in Informatics. Gesellschaft für Informatik. Bonn, S. 2149–2166.

42 Steinmüller warnte schon früh vor dieser Möglichkeit und verlangte daher, dass auch statistische Informationen dem Datenschutzrecht unterworfen werden, siehe Wilhelm Steinmüller (1971). „Allgemeine Grundsätze zur rechtlichen Regelung des Datenschutzes". In: Datenschutz – Datensicherung. Hrsg. von Jochen Schneider. Beiträge zur integrierten Datenverarbeitung in der öffentlichen Verwaltung Heft 5. München: Siemens Aktiengesellschaft. Kap. 3, S. 13–17, S. 16.

43 Für die Schwierigkeiten, ein als Gefahrenabwehr wirkendes Schutzrecht ausschließlich auf Verwendungsbeschränkungen zu gründen, und die umfassende Diskussion in den 1960er Jahren dazu, siehe Arthur Raphael Miller (1969). „Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society". In: Michigan Law Review 67.6, S. 1089–1246.

44 Adalbert Podlech (1982). „Individualdatenschutz – Systemdatenschutz". In: Beiträge zum Sozialrecht – Festgabe für Grüner. Hrsg. von Klaus Brückner und Gerhard Dalichau. Percha: Verlag R. S. Schulz, S. 451–462, S. 452.

45 Vgl. Pohle 2014a, S. 51 f.

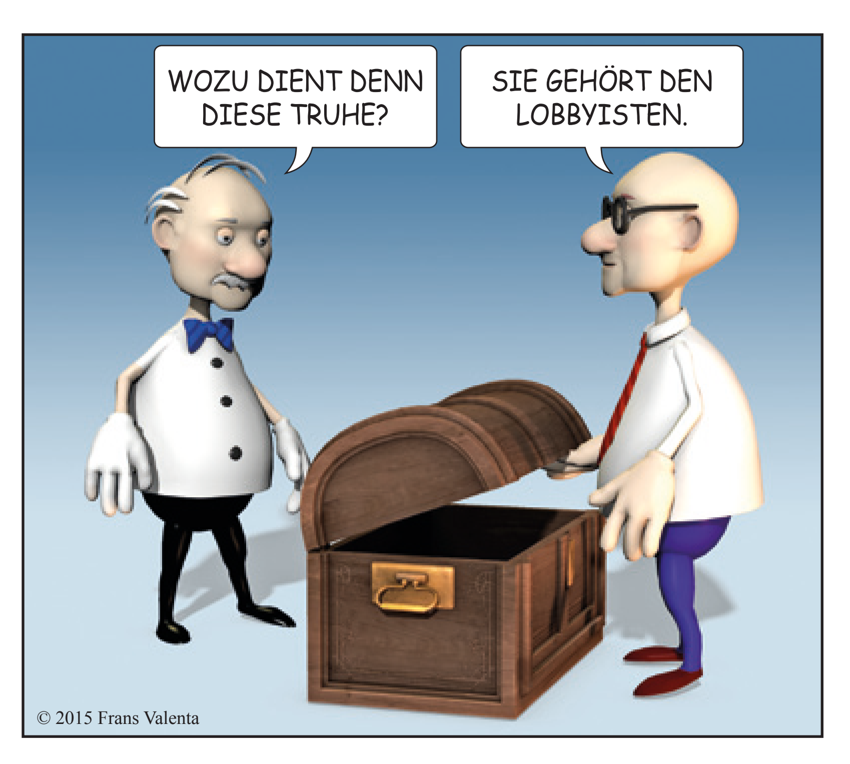
46 Vgl. Gabriela Zanfir (2013). Forgetting about consent. Why the focus should be on „suitable safeguards" in data protection law. University of Craiova. Faculty of Law und Adminsitrative Sciences.

47 Grundlegend Martin Rost und Andreas Pfitzmann (2009). „Datenschutz-Schutzziele – revisited". In: Datenschutz und Datensicherheit 33.6, S. 353–358.

48 Vgl. Marit Hansen, Meiko Jensen und Martin Rost (2015). „Protection Goals for Privacy Engineering". In: 2015 International Workshop on Privacy Engineering (IWPE). IEEE eXplore.

49 Vgl. etwa Martin Eifert (2007). „Zweckvereinbarkeit statt Zweckbindung als Baustein eines modernisierten Datenschutzes". In: Rechtswissenschaft im Wandel. Hrsg. von Walter Gropp, Martin Lipp und Heinhard Steiger. Tübingen: Mohr Siebeck, S. 139–152.

Cartoon





Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Minister nutzen vermehrt Wegwerf-Handys

Hohe deutsche Beamte und Mitglieder der Bundesregierung nutzen auf ihren Dienstreisen offenbar immer häufiger Einweg-Handys, weil sie Angst davor haben, ausgespäht zu werden. Die Gefahr durch ausländische Agenten ist real. Bei offiziellen Auslandsreisen werden die Einweg-Handys nach der Rückkehr nach Deutschland vernichtet, und dies nicht nur bei Reisen nach China und Russland, sondern auch in verbündete Staaten wie Großbritannien und die USA.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hatte Bundesminister, Staatssekretäre und andere hochrangige Regierungsbeamte schon vor etwa zehn Jahren davor gewarnt, ihre eigenen Mobiltelefone mit auf Reisen zu nehmen. Da diese vor vertraulichen Gesprächen oft abgegeben werden müssten, bestehe die Gefahr einer Manipulation, etwa durch das heimliche Aufspielen einer Spionagesoftware. Es sei ratsam, so das BSI in einem Merkblatt, ein unbenutztes Handy mitzunehmen und darauf nur die nötigsten Daten zu übertragen. Diese Mahnung war offenbar lange Zeit vielfach in den Wind geschlagen worden, so ein Pressebericht, der Sicherheitskreise zitiert: „Es gibt deutliche Signale, dass man sensibler geworden ist.“ Nicht alle Regierungsmitglieder folgen dem BSI-Ratschlag. So seien Außenminister Frank-Walter Steinmeier und Wirtschaftsminister Sigmar Gabriel (beide SPD) zuletzt mit ihren eigenen Mobiltelefonen nach Kuba und China geflogen. In ihrem Umfeld hieß es, die Minister achteten darauf, dass ihre Handys nicht in fremde Hände geraten (Der Spiegel 30/2015, 18; Regierungsmitglieder nutzen vermehrt Wegwerf-Handys, www.rp-online.de 18.07.2015).

Bund

Lufthansa will mit Kundendaten Geld verdienen

Auf der Suche nach neuen Erlösquellen will die Lufthansa mit den Daten ihrer Fluggäste Geld verdienen. Lufthansa-Finanzvorstand Simone Menne meinte, Fliegen allein bringe es nicht mehr: „Nach Umsatz sind wir der größte Luftfahrt-Konzern der Welt. Aber die Märkte bewerten Google, Whatsapp nach ganz anderen Maßstäben – nur dank der Daten, die sie generieren. Unsere Kundendaten dagegen werden an der Börse überhaupt nicht bewertet, folglich müssen wir mehr daraus machen. Wir müssen arbeiten mit diesen Daten.“ Ein Lufthansasprecher sagte, es liefen diverse Projekte, „um mit Kundendaten Zusatzerlöse zu generieren, etwa mit individuellen Angeboten“. Es gehe aber nicht darum, Daten zu verkaufen (Lufthansa will mit Kundendaten Geld verdienen, www.welt.de 13.06.2015; Lufthansa will Geld mit Kundendaten verdienen, SZ 15.06.2015, 20).

Nordrhein-Westfalen

Helga Block wird neue Datenschutzbeauftragte

Die Landesregierung Nordrhein-Westfalen hat auf Vorschlag des Ministers für Inneres und Kommunales beschlossen, dem nordrhein-westfälischen Landtag Ministerialdirigentin Helga Block als neue Landesbeauftragte für Datenschutz und Informationsfreiheit (LDI) zur Wahl vorzuschlagen. Innenminister Ralf Jäger erklärte am 16.06.2015 in Düsseldorf: „Aus meiner Sicht ist Frau Block die richtige Wahl, um auch zukünftig über den Schutz von Daten zu wachen und die Freiheit beim Zugang zu Informationen in Nordrhein-Westfalen zu verwirklichen.“ Helga Block tritt die Nachfolge des 1950 geborenen Ulrich Lepper an, der Ende September 2015 nach fünf Jahren als oberster Datenschützer in den Ruhestand tritt.

Seit 2001 war die gebürtige Münsteranerin als Abteilungsleiterin im Innenressort unter anderem für die Themen Verfassungsrecht und Datenschutz verantwortlich. Zudem ist sie Landeswahlleiterin des Landes Nordrhein-Westfalen. Die Juristin arbeitete zunächst in den Bezirksregierungen in Detmold und Düsseldorf. Seit 1989 ist sie mit einer zweijährigen Unterbrechung im damaligen Ministerium für die Gleichstellung von Frau und Mann in verschiedenen Positionen im Innenministerium tätig.

Die Stelle der bzw. des LDI überwacht die Einhaltung der Datenschutzvorschriften bei den öffentlichen und nicht-öffentlichen Stellen und gibt diesen gegenüber Empfehlungen. Sie ist für die Sicherstellung des Rechts auf Information zuständig und Anlaufstelle für Bürgerinnen und Bürger bei Fragen zum Datenschutz und zur Informationsfreiheit (Helga Block soll neue Datenschutzbeauftragte werden, https://land.nrw/de 16.06.2015).

Rheinland-Pfalz

Kugelmann folgt Wagner

Die Fraktionen von SPD und Grünen haben sich in Rheinland-Pfalz auf Prof. Dr. Dieter Kugelmann als neuen Datenschutzbeauftragten geeinigt, der die Nachfolge von Edgar Wagner antritt, dessen Amtszeit eigentlich schon am 15.04.2015 zu Ende gewesen wäre. Kugelmann wurde vom Landtag Rheinland-Pfalz am 01.07.2015 gewählt. Er übernimmt das Amt am 01.10.2015. Der SPD-Fraktionsvorsitzende Alexander Schweitzer erklärte: „Mit Dieter Kugelmann haben die Koalitionsfrakti-

onen eine Persönlichkeit nominiert, die hervorragend geeignet ist als Sachwalter von Datenschutzinteressen." Sein Kollege Daniel Köbler von den Grünen ergänzte, mit Kugelmann gewinne Rheinland-Pfalz einen anerkannten Rechtswissenschaftler mit einem Schwerpunkt auf Informationsfreiheit.

Der 52-jährige Kugelmann wurde im pfälzischen Landau geboren und studierte unter anderem in Mainz Jura. 2006 trat er eine Professur an der Hochschule Halberstadt an, ehe er 2008 zum Professor für Öffentliches Recht und Polizeirecht an der Deutschen Polizeihochschule in Münster ernannt wurde. Kugelmann hat sich als Wissenschaftler unter anderem mit dem Informationsfreiheitsgesetz des Bundes beschäftigt. Kugelmann stellte sich am 03.06.2015 den Regierungsfraktionen von SPD und Grünen vor. Bei beiden Terminen soll er große Zustimmung erhalten haben.

Wagner meinte rückblickend: „Dieses Amt ist klasse." Aber er sieht auch die Notwendigkeit für einen Generationenwechsel: „Ich bin aus einer anderen Generation, aus der Generation Münzfernsprecher." Er nutzte seine Verabschiedung, um Kritik an der geplanten Vorratsdatenspeicherung zu üben. „Dass die Koalitionsfraktionen im Bund sich wieder darauf einlassen, die Grenzen der Verfassung auszuloten, halte ich für sehr problematisch. Wenn man sich überhaupt auf eine Vorratsdatenspeicherung einlassen will, dann sollte sie eng begrenzt werden." Auch Nachfolger Kugelmann soll sich bei seiner Vorstellung bei den Fraktionen kritisch über die Speicherung der Vorratsdaten gezeigt haben. Ministerpräsidentin Malu Dreyer (SPD) forderte im Rahmen von Wagners Verabschiedung eine lückenlose und zügige Aufklärung der Spähaffäre um den US-Geheimdienst NSA. Sie habe Kanzlerin Angela Merkel (CDU) einen Brief geschrieben, um zu erfahren, welche rheinland-pfälzische Firmen betroffen seien. Wagner nannte sie einen Streiter für die Rechte der Menschen (Kugelmann folgt auf Wagner, www.swr.de 03.06.2015; LfDI RhPf. PM 01.07.2015, Prof. Dr. Dieter Kugelmann zum neuen Landesbeauftragten für den Datenschutz und die Informationsfreiheit gewählt).

Schleswig-Holstein

Marit Hansen folgt Thilo Weichert im ULD

Am 15.07.2015 wählte der Schleswig-Holsteinische Landtag Marit Hansen zur dortigen Landesbeauftragten für Datenschutz. Marit Hansen war seit 2008 die Stellvertreterin von Dr. Thilo Weichert, der über zwei Amtsperioden das Amt des Landesbeauftragten für Datenschutz ausgefüllt hat und davor ebenfalls als Stellvertreter tätig war. Nach insgesamt 17-jähriger Arbeit für die Datenschutzbehörde verlässt er nun das Unabhängige Landeszentrum für Datenschutz (ULD). In seiner Amtszeit entwickelten sich soziale Netzwerke, Web 2.0, Cloud Computing und Big Data, deren Datenschutzfragen er als einer der ersten in Publikationen und Vorträgen behandelte. Mit seiner Dienststelle ermittelte er in mehreren Datenschutzskandalen, wie beispielsweise dem Missbrauch von Kontodaten durch Call-Center.

Mit Marit Hansen wird das erste Mal in Deutschland eine Informatikerin Datenschutzbeauftragte. Nach ihrem Studium an der Christian-Albrechts-Universität zu Kiel spezialisierte sie sich auf Datenschutz. Zu ihren Schwerpunkten im ULD gehört die Konzeption und Gestaltung von rechtskonformen und technisch realisierbaren Lösungen. Seit 20 Jahren arbeitet die gebürtige Schleswig-Holsteinerin an der Schnittstelle von Jura und Informatik mit dem Ziel, Datenschutz handhabbar zu machen und von Anfang an in die Systeme einzubauen. Die Kompetenz der parteilosen Datenschützerin wird von der Wirtschaft, von nationalen und internationalen Forschungsteams sowie europäischen Projektkonsortien nachgefragt.

Die 46-Jährige steht für inhaltliche Kontinuität der Arbeit des ULD und wird die bewährten Instrumente von Kontrolle, Prüfung und Beratung über Aus- und Fortbildung, Audit und Gütesiegel bis hin zum Bereich innovativer Datenschutzprojekte fortführen und ausgestalten. Das ULD bleibt weiterhin Servicezentrum zu Datenschutz und Informationsfreiheit. Dabei unterstützt es schleswig-holsteinische Bürgerinnen und Bürger ebenso wie die Verwaltung und die Wirtschaft und geht Verstößen gegen das Recht nach (PM ULD SH 15.07.2015, Marit Hansen zur Landesbeauftragten für Datenschutz Schleswig-Holstein gewählt, www.datenschutzzentrum.de).

Datenschutznachrichten aus dem Ausland

Europa

Nach Germanwings-Unglück: Expertengruppe für bessere medizinische Kontrolle

Eine Expertengruppe unter Vorsitz der europäischen Flugsicherheitsbehörde EASA hat Konsequenzen aus dem Germanwings-Unglück am 24.03.2015 vorgeschlagen (vgl. DANA 2/2015, 82). Transportkommissarin Violeta Bulc hatte die Taskforce nach dem Unglück ins Leben gerufen, der auch der für den Flugbetrieb zuständige Bereichsvorstand des Lufthansa-Konzerns Kay Kratky angehörte. Deren Bericht soll als Grundlage für spätere Empfehlungen an die Flugbranche und für mögliche Gesetzesänderungen dienen. Die Fachleute fordern generelle psychologische Untersuchungen für künftige BerufspilotInnen: „Derzeit gibt es angehende Berufspiloten, die für ihre Ausbildung niemals eine psychologische Bewertung absolvieren." Zwar müssten sich Flugmediziner auf die Angaben der PilotInnen zu möglichen Gesundheitsproblemen

verlassen können, doch solle mehr Wert auf die psychologischen Qualifikationen der ÄrztInnen gelegt werden. Weiterhin werden Alkohol- und Drogentests stichprobenartig und bei besonderen Anlässen durchführen. Der German-Wings-Unglückspilot Andreas Lubitz hatte offensichtlich zeitweise starke Antidepressiva genommen, die bei Untersuchungen auch noch im Nachhinein gefunden worden wären. Die Unternehmen müssten unterscheiden zwischen „solider Unterstützung für Piloten, die (Probleme) selbst melden und Intoleranz für Piloten, die sich nicht melden und ihr eigenes und das Leben anderer in Gefahr bringen".

Die Qualifikation und die Leistung von FliegerärztInnen sollen künftig besser überprüft werden. Die EASA könnte hier neue Standards entwickeln. Zudem sollten sich diese ExpertInnen europaweit stärker vernetzen. Es wird ein „Gleichgewicht zwischen Arztgeheimnis und Flugsicherheit" gefordert: Angehende PilotInnen können sich medizinische Atteste in jedem europäischen Staat ausstellen lassen, der EASA-Mitglied ist. Dazu gehören neben den 28 EU-Ländern etwa die Schweiz oder Island. PilotInnen könnten daher „Medizin-Tourismus" betreiben und Staaten ohne zentrales System zur Datenspeicherung wählen. Zudem könnten sie FlugmedizinerInnen konsultieren, die im Ruf stehen, weniger streng zu sein. Grunddaten zu bestimmten Untersuchungen sollten daher für ganz Europa zusammengeführt werden. Dabei soll es vorerst nur um Personendaten von PilotIn und ÄrztIn, aber nicht um medizinische Informationen gehen. Die Autoren des Berichts betonen, dass das Arbeitsumfeld die PilotInnen bestmöglich unterstützen soll. Vertrauen zu den KollegInnen und zum Arbeitgeber sei wichtig, um Probleme frühzeitig ansprechen zu können. Eine „Atmosphäre der Angst" müsse vermieden werden.

Der Germanwings-Mutterkonzern Lufthansa lobte die EU-Empfehlungen zur Flugsicherheit. Die in Brüssel vorgestellten Vorschläge stünden im Einklang mit den Ergebnissen der deutschen Expertengruppe von Bundesregierung und dem Luftverkehrsverband BDL, erklärte das Unternehmen am 17.07.2015 in Frankfurt. Einzelne Punkte wie zum Beispiel die Anlaufstellen für Crewmitglieder seien bei Lufthansa bereits seit vielen Jahren etabliert (Flottau, Strenger Blick ins Cockpit, SZ 18./19.07.2015, 6; EU-Arbeitsgruppe will psychologische Test für Piloten, www.tagesspiegel.de 17.07.2015).

Großbritannien

Clooneys Überwachungskameras bedrohen Nachbarn

Der US-amerikanische Schauspieler und Regisseur George Clooney hat Probleme mit der Bauvorschriften in England, der Heimat der Anwältin Amal Alamuddin, die er 2014 geheiratet hat, und wo er im schönen Oxfordshire ein denkmalgeschütztes Anwesen aus dem 17. Jahrhundert erwarb. Ein Schwimmbecken und die Einrichtung eines Kinosaals waren noch kein Problem. Doch als das Ehepaar Clooney 18 schwenkbare Überwachungskameras im weitläufigen Gelände auf bis zu sechs Meter hohen Masten anbringen wollte, um das Anwesen gegen unerwünschte Eindringlinge zu schützen, stieß er auf Widerstand des zuständigen Gemeindeparlaments: Derart hohe Pfeiler würden nicht zu einem denkmalgeschützten Anwesen passen. Außerdem könnten die Kameras von hoch oben aus Nachbarn filmen und deren Privatsphäre stören. Die Ratsherren schlugen vor, stattdessen lieber mehr Kameras zu nutzen und diese an niedrigeren Positionen anzubringen (George Clooney liebt Kameras – zu sehr, SZ 23.07.2015, 16).

Kanada – weltweit

Hacker stellen Seitensprungdaten ins Netz und drohen

Nach einem Hacker-Einbruch sind KundInnendaten der Seitensprungagentur Ashley Madison im Netz aufgetaucht. Gemäß einem Bericht des renommierten Sicherheitsexperten Brian Krebs ist der Betreiber des Seitensprungportals, der kanadische Internet-Konzern Avid Life Media (ALM), Opfer eines Datendiebstahls geworden. Die Hacker sollen dabei unter anderem die Nutzerdaten von Ashley Madison und anderen Sites des Konzerns erbeutet haben. Alleine Ashley Madison hat nach Angaben eines Unternehmenssprechers weltweit 37 Millionen Mitglieder und ist auch im deutschsprachigen Raum aktiv. Bei den veröffentlichten Daten handelt es sich u. a. um Informationen zu Gehältern und Bankkonten von ALM. Ebenso seien aber Daten-Schnipsel zu Nutzer-Accounts von Ashley Madison und zwei weiteren ALM-Portalen online aufgetaucht.

Zu der Veröffentlichung der Seitensprungdaten soll sich eine Person oder eine Gruppe mit dem Pseudonym „The Impact Team" bekannt haben. Laut Krebs wirft „The Impact Team" ALM vor, ihre KundInnen wegen ihrer Löschpraktiken anzulügen. In seiner Stellungnahme behauptet „The Impact Team", Zugang zu allen Kundendatenbanken zu haben und fordert ALM auf, Ashley Madison und ein weiteres Portal aus dem Netz zu nehmen. Ashley Madison offline zu nehmen, werde das Unternehmen etwas kosten, heißt es, „aber wenn ihr euch weigert, wird euch das noch mehr kosten". Falls ALM der Forderung nicht nachkomme, werde man alle Daten aller KundInnen inklusive Sexfantasien, Nacktfotos und Gesprächen online stellen, ebenso Informationen zu Kreditkarten und echten Namen und Adressen.

Der Geschäftsführer von ALM Noel Biderman bestätigte den Vorfall: „Aber, ob man uns mag oder nicht, es handelt sich um eine Straftat." Das Seitensprungportal will nach dem großen Datendiebstahl seine umstrittene Politik zur Löschung von Anwender-Profilen ändern. Bislang hatte Ashley Madison 19 US-Dollar von seinen KundInnen verlangt, die ihr Konto inklusive der über die Plattform ausgetauschten Mitteilungen und Bilder endgültig löschen wollten. Jetzt will das Unternehmen die Lösch-Option für alle Mitglieder kostenlos anbieten. Sicherheitsexperte Graham Cluley kritisierte den Schritt: „Die schließen das Tor, nachdem das Pferd bereits aus der Scheune abgehauen ist". Avid Life Media wies Berichte zurück, das bezahlpflichtige Löschangebot sei technisch nie umgesetzt worden. Nach einer Löschanfrage würden tatsäch-

lich das komplette Mitgliederprofil und sämtliche Kommunikationsaktivitäten gelöscht. Dazu gehören Bilder und Nachrichten an andere Mitglieder der Plattform.

Vor Ashley Madison war bereits ein anderes großes Portal für Sexkontakte von einem Datenleck betroffen: Im Mai 2015 war eine zwei Monate zuvor erfolgte Attacke auf AdultFriendFinder bekannt geworden, bei der 3,5 Mio. Konten betroffen waren. Damals waren Datensätze ins Netz gestellt worden, in denen sich nicht nur E-Mail-Adressen, Geburtsdatum, Postleitzahl sondern auch private Angaben fanden, etwa zu sexuellen Vorlieben der Mitglieder des Portals. Von dem Datendiebstahl waren anscheinend auch Mitglieder betroffen, die ihre Profile gelöscht hatten. In einem Obline-Forum hatten daraufhin Unbekannte gedroht, die Daten für Spam-Attacken zu nutzen. AdultFriendFinder ist schon 1996 als Kontaktbörse für Sexualpartner gegründet worden und hat nach eigenen Angaben mehr als 40 Mio. Nutzende. Der Mutterkonzern FriendFinder Networks Inc. teilte auf seiner Webseite mit, man arbeite eng mit den Strafverfolgungsbehörden zusammen (Ashley Madison: Nach Hackerattacke bietet das Seitensprungportal kostenlose Datenlöschung an, www.heise.de 21.07.2015; Unbekannte stellen Daten von Seitensprungportal ins Netz www.manager-magazin.de 20.07.2015; Mosbergen, Hackers Threaten To Out 37 Million Users Of Cheating Website AshleyMadison.com 20.07.2015; US-Sexpartnerbörse gehackt, SZ 23.-25.05.2015, 28).

USA

Hacker stehlen Millionen Personaldatensätze von Verwaltung

Anfang Juni 2015 wurde ein erfolgreicher Hackerangriff auf Personaldaten der US-Regierung bekannt. Als die Personalverwaltung am 04.06. einen erfolgreichen Hackangriff auf das Personalbüro der US-Bundesbehörden (Office of Personnel Management – OPM) entdeckte, erklärte sie, dass die Personaldaten von 4 Millionen Menschen kompromittiert wurden. Tatsächlich war das Ausmaß aber viel schlimmer. Später teilte die Regierung mit, dass 18 Mio. Personalakten erbeutet worden sind.

Der angeblich zweite Hack betrifft Informationen, die im Rahmen von Sicherheitsüberprüfungen (Security Clearances) über Personen und ihr Umfeld gesammelt wurden. Wieviele Personen genau betroffen sind, wusste OPM nicht, wie aus einem Brief der OPM-Direktorin Katherine Archuleta vom 24.06.2015 hervorgeht. Sie wendet sich darin an den Abgeordneten im Repräsentantenhaus Jason Chaffetz. Der Republikaner ist Vorsitzender des Ausschusses, der für die Überprüfung der Verwaltung zuständig ist. Chaffetz hat Archuleta bereits zum Rücktritt aufgefordert, was sie aber ablehnt.

Die in US-Medien genannte Zahl von 18 Millionen Sozialversicherungsnummern aus den Sicherheitsüberprüfungen, so Archuleta in ihrem Brief, sei eine „vorläufige, nicht verifizierte, ungefähre“ Angabe. Da die Sicherheitsüberprüfung eines Menschen naturgemäß die Überprüfung seines persönlichen Umfelds nötig macht, dürften die Hacker Angaben über eine vielfach größere Gruppe als die 18 Millionen Bürger plus 4,2 Millionen Mitarbeiter erbeutet haben. Archuleta weiter: „Außerdem arbeiten wir bewusst daran, festzustellen, ob Personen, deren Sozialversicherungsnummern nicht kompromittiert wurden, über die aber andere Informationen preisgegeben worden sein könnten, auch als Betroffene des Vorfalls betrachtet werden sollten.“ Die 18 Millionen hatten für eine Bundesbehörde gearbeitet oder arbeiten wollen, beziehungsweise waren im Auftrag eines anderen (potenziellen) Arbeitgebers überprüft worden. Betroffen sind auch verdeckte Ermittler, deren falsche Identität nun auf dem Spiel steht. Ein Datenexperte nennt den Datendiebstahl einen „Raub der Kronjuwelen“, Lottogewinn für jeden feindlichen Nachrichtendienst. Alles, was Spione und Agenten in Zeiten des Kalten Krieges in mühsamer Kleinarbeit zusammentragen mussten, könne jetzt auf Knopfdruck heruntergeladen werden. Gemäß einem Nachrichtenportal sind auch die Daten von FBI-Direktor James Comey betroffen, der sich wie folgt äußerte: „Wenn dem so ist, kennt man nun jeden Ort, an dem ich gelebt habe, seit ich 18 Jahre alt bin, jeden Nachbarn, alle Menschen, mit denen ich beruflich zu tun hatte, alle meine Reisen ins Ausland.“ Laut US-Regierungskreisen soll der Hack von der Volksrepublik China ausgehen, die das aber in Abrede stellt. Dies seien „grundlose Anschuldigungen“.

Am 09.07.2015 musste Archuleta ein weiteres Mal persönlich vor dem Ausschuss aussagen. Dabei gestand sie ein, dass „aufgrund des Alters unserer Einrichtungen Verschlüsselung [gespeicherter Daten] nicht immer möglich“ sei. Bei dem Angriff hätte eine Verschlüsselung aber sowieso nichts gebracht. Die Angreifer hätten dann auch die Schlüssel und Passwörter kopiert. 2014 hatte das interne Aufsichtsbüro des OPM empfohlen, 11 seiner 47 IT-Systeme stillzulegen, die keine gültigen Sicherheitsbescheinigungen mehr hatten. Das OPM folgte der Empfehlung nicht. „Systeme abzuschalten würde bedeuten, dass Rentner nicht bezahlt werden, und dass keine neuen Sicherheitsbescheinigungen ausgestellt werden könnten“, rechtfertigte sich Archuleta. Inzwischen hätten 10 der 11 Systeme eine neue oder zumindest eine eingeschränkte Sicherheitsbescheinigung erhalten.

Die Presse warf OPM nicht nur vor, in Absprache mit dem Weißen Haus den Hack in zwei Vorfälle geteilt, sondern auch, die Preisgabe der Sicherheitsdaten zweimal geleugnet zu haben. Journalisten hatten konkret nach den Daten aus den Sicherheitsüberprüfungen gefragt: Einmal vor der Bekanntmachung des „ersten Vorfalls“ durch das OPM, und dann erneut am Tag danach. Bei der zweiten Leugnung habe das FBI das OPM jedoch bereits über die Zugriffe auf die Sicherheitsinformationen informiert gehabt. Und auch gut vernetzte Außenstehende wussten offenbar bereits Bescheid. Aus einem Rundschreiben der Präsidentin der Universitäten von Kalifornien vom 05.06. geht hervor, dass sie von der Kompromittierung der Sicherheitsüberprüfung wusste. Die Uni-Präsidentin heißt Janet Napolitano und war bis September 2013 Ministerin für Heimatschutz (Batthyany, Raub der digitalen Kronjuwelen, SZ 11./12.07.2015, 9; Hack des Personalbüros der US-Regierung viel schlimmer als gedacht, www.heise.de 25.06.2015).

USA

Nach Verhöhnung bei Operation 1/2 Mio. Dollar Schadenersatz

Eine US-Ärztin in Vienna/Virginia lästerte 2013 während der Operation über den Patienten, der narkotisiert vor ihr lag: „Syphilis am Arm", „Tuberkulose am Penis". Sie wusste nicht, dass das Smartphone des Mannes die gesamte Behandlung akustisch aufzeichnete – einschließlich aller Beleidigungen. Dies wurde teuer. Der Patient wollte lediglich die Anweisungen der Ärzte aufnehmen, die sie ihm nach seiner Darmspiegelung geben würden. Deshalb drückte er vor seiner Behandlung die „Aufnahme"-Taste auf seinem Smartphone. Als der Patient aus Reston im US-Bundesstaat Virginia allerdings auf seinem Weg nach Hause die Aufnahme abspielte, traute er seinen Ohren nicht. Der Patient hatte versehentlich die gesamte Operation mitgeschnitten – und dabei auch diverse Lästereien und Beleidigungen seitens des Operationsteams eingefangen.

Die „Washington Post" veröffentlichte Teile der Mitschnitte auf ihrer Webseite: „Während unseres OP-Vorgesprächs wollte ich Dir nach fünf Minuten ins Gesicht schlagen und Dich ein bisschen aufmischen", so die 42-jährige Anästhesistin während der Behandlung im Audio-Mitschnitt. Weiter warnte sie eine Kollegin davor, ihre Schutzkleidung abzulegen und besser nicht mit dem Mann in Berührung kommen. Sonst könne sie „Syphilis oder so etwas am Arm bekommen". Anschließend fügte sie unter Gelächter hinzu: „Es ist wahrscheinlich Tuberkulose am Penis, also wird Dir nichts passieren." Kurze Zeit später hört man die Ärztin weiter über den Patienten spotten. Diesem werde nach eigenen Angaben schlecht, wenn er dabei zusieht, wie man ihm eine Nadel in den Arm sticht. „Na, warum siehst Du dann hin, Vollidiot?", höhnte die Ärztin. Der Gastroenterologe ließ es sich nicht nehmen, einen Kommentar zu dem schlafenden Mann abzugeben. „Solange es nicht Ebola ist, ist es okay."

Das Operations-Team wusste nicht, dass in der Hose des Patienten, die direkt unter dem Operationstisch lag, sich sein Smartphone befand, welches jedes Wort mitschnitt. Die Aufnahmen belegen, dass die MedizinerInnen darüber redeten, wie sie dem Mann nach der Behandlung aus dem Weg gehen könnten. Eine Krankenschwester sollte sich diesbezüglich einer Lüge bedienen. Schließlich teilte die Anästhesistin mit, dass sie im Befund „Hämorrhoiden" angeben werde, obwohl gar keine gefunden worden wären, als „Ein Schuss ins Blaue." Das soll sie dann auch tatsächlich gemacht haben.

Der Patient ließ sich das Verhalten nicht gefallen und zog 2014 mit dem Audio-Material gegen zwei Ärzte vor Gericht und forderte 5 Mio. Dollar Schadenersatz. Tatsächlich bekam er 500.000 Dollar (rund 445.000 Euro) zugesprochen: jeweils 50.000 Dollar für den Syphilis- und den Tuberkulose-Kommentar wegen Diffamierung, 200.000 Dollar wegen ärztlicher Behandlungsfehler und 200.000 Dollar zusätzlicher Schadenersatz. Gemäß einem Pressebericht meinte einer der Geschworenen: „Wir kamen schließlich zu dem Schluss, dass wir ihm etwas geben müssen. Einfach um sicherzustellen, dass so etwas nicht wieder passiert" (Ärztin beleidigt Patienten in Narkose – sein Handy nahm alles auf, www.focus.de 25.06.2015; Ärzte-Trashtalk, SZ 26.06.2015, 10).

Rechtsprechung

EGMR

Forenbetreiber haftet für Beleidigungen durch Nutzende

Der Europäische Gerichtshof für Menschenrechte (EGMR) in Straßburg entschied am 16.06.2015, dass ein Betroffener einer Beleidigung im Webforum eines kommerziellen Anbieters von diesem Forenbetreiber Schadensersatz fordern kann, selbst wenn der die entsprechenden Posts auf Wunsch bereits entfernt hat. Ausgangspunkt war ein Streit darüber, ob in Estland Fähren vor der Küste das Eis kaputt machen dürfen. Das estnische Nachrichtenportal Delfi.ee hatte den EGMR angerufen. Auf der Plattform war im Januar 2006 ein Artikel über eine estnische Fährgesellschaft erschienen: Das Unternehmen hatte seine Routen zu bestimmten Inseln geändert. Dies führte dazu, dass die Fähren das Eis an Stellen zerbrachen, an denen eigentlich Eisstraßen hätten angelegt werden sollen. Solche Eisstraßen ermöglichen Inselbewohnern, ohne Fähre nach Hause zu kommen – mit dem eigenen Auto übers Eis. Die Schäden durch die Fähren verzögerten die Entstehung der Eisstraßen um mehrere Wochen.

Für manche Esten war das Thema ein ausgesprochen emotionales, wie man an den Kommentaren unter dem betreffenden Delfi.ee-Artikel sehen kann. Vertreter der Fährgesellschaft wurden teils wüst beschimpft, es fielen Begriffe wie „Abschaum", „Schweine" und „Bastard". Auch Aufrufe zur Gewalt gegen den Besitzer der Firma gab es. Delfi.ee entfernte die beleidigenden Kommentare nach entsprechenden Hinweisen. Doch der Besitzer des Fährunternehmens, dessen Name von einigen der wütenden Kommentatoren genannt worden war, war damit nicht zufrieden und verklagte das Nachrichtenportal Delfi vor einem Zivilgericht auf eine Entschädigung. Gegen eben jene

Entschädigungsforderung ging Delfi.ee nun seinerseits vor – und unterlag. Nach Ansicht des EGMR hatte Delfi die anstößigen Kommentare nicht schnell genug entfernt. Das Gericht betont, dass es hier um ein kommerzielles Nachrichtenangebot gehe, und nicht um „andere Foren im Internet, wo von Dritten Kommentare verbreitet werden können, zum Beispiel ein Internetdiskussionsforum, ein Bulletin Board oder eine Social-Media-Plattform".

Schon im Oktober 2013 hatte der EGMR einmal gegen die Nachrichtenseite entschieden (Az.: 64569/09). Das Gericht entschied damals, dass die gegen Delfi verhängte Schadensersatzzahlung in Höhe von etwa 320 Euro nicht als Einschränkung der Meinungsfreiheit zu werten sei. Diese Urteil wurde jedoch nicht rechtskräftig, der Fall wurde stattdessen an die Große Kammer des EGMR verwiesen, welche die Entscheidung bekräftigte.

Der Fall hat Relevanz für Betreiber von kommerziellen Nachrichtenangeboten in allen 47 Ländern des Europarats. Sie müssen sich darauf gefasst machen, für bösartige oder diffamierende Kommentare anonymer Nutzender unter Umständen zur Rechenschaft gezogen zu werden. Dies gilt für alle EU-Länder, für die Schweiz, die Türkei und die meisten osteuropäischen Länder wie Russland und die Ukraine, die Mitglieder der Straßburger Staatenorganisation sind. In Deutschland kann die Polizei bei Verleumdungen oder Beleidigungen verlangen, dass Seitenbetreiber die IP-Adresse der Nutzer offenlegen.

Webseitenbetreiber haften unter Umständen für rechtsverletzende Beiträge ihrer Nutzer in Kommentarspalten, etwa, wenn ein Beitrag beleidigend ist oder unwahre Tatsachenbehauptungen enthält. Wird ein Webseitenbetreiber auf solche Inhalte hingewiesen – ob per Kontaktformular, Meldefunktion, Mail oder über sonstige Kanäle, muss er nach den Grundsätzen der sogenannten Störerhaftung reagieren und beanstandete Beiträge gegebenenfalls löschen. Kommt er Beschwerden nicht innerhalb einer angemessenen Frist nach, drohen wegen der Verbreitung des Beitrags Unterlassungsansprüche und teure Abmahnungen. Ebenso muss ein Webseitenbetreiber angemessene Maßnahmen ergreifen, um zu verhindern, dass derselbe oder ein vergleichbarer Kommentar nicht einfach wieder in das Kommentarforum eingestellt wird. Was eine „angemessene" Frist ist, und was als „angemessene" Maßnahme gegen eine Wiederveröffentlichung gilt, ist bisher nicht eindeutig definiert. Werden auf der eigenen Webseite Kommentare zugelassen, sollte man in der Lage sein, schnell zu reagieren. Bei veröffentlichten Tatsachenbehauptungen ist es jedoch oft schwierig, deren Wahrheitsgehalt zu überprüfen und zu beweisen. Kann man das nicht, sollte man vorsorglich den Beitrag löschen, um weiteren Ärger zu vermeiden.

Auch Verfasser rechtsverletzender Kommentare müssen mit Schwierigkeiten rechnen, wenn sich Betroffene beschweren. Deswegen sollte man besonders mit Tatsachenbehauptungen vorsichtig sein. Auch Werturteile sollten stets einen Sachbezug aufweisen (Forenbetreiber haftet für Beleidigungen der Nutzer www.spiegel.de 16.06.2015).

EuGH

Markenrechte vor Datenschutz

Der Europäische Gerichtshof (EuGH) in Luxemburg hat mit Urteil vom 16.07.2015 das Bankgeheimnis bei Internetstraftaten gelockert. Werden auf Internetplattformen gefälschte Waren verkauft, können geschädigte Rechteinhaber von der Bank Auskunft über den Konteninhaber verlangen (Az. C-580/139). Den Ausgangsfall hatte die deutsche Firma Coty Germany angestoßen, die Lizenzinhaberin des Parfums Davidoff Hot Water ist. Sie verlangte von der Sparkasse Magdeburg Auskunft über einen Konteninhaber, der auf einer Internetplattform Fälschungen des Parfums angeboten hatte. Die Sparkasse verweigerte die Auskunft unter Berufung auf das Bankgeheimnis. Der damit befasste Bundesgerichtshof (BGH) legte den Fall dem EuGH vor. Die Luxemburger Richter entschieden, dass das Recht des geistigen Eigentums in solchen Fällen stärker wiegt als der Schutz personenbezogener Daten. Banken und Sparkassen können sich demnach insofern nicht auf ihr Bankgeheimnis berufen (EuGH lockert Bankgeheimnis bei Internetstraftaten, www.freenet.de 16.07.2015).

Unterwegs und überwacht

Datenschutztagung 09. + 10.10.2015 in Bonn

- Was weiß mein Auto über mich?
- Mit wem spricht mein Auto?
- Was verraten meine Mobilitätsdaten?

Tagungsprogramm und Anmeldung unter www.datenschutzverein.de
oder bei DVD, Reuterstraße 157, 53113 Bonn • 0228 / 24 202 78

Die Veranstaltung wird unterstützt von: IG Metall · FORBIT

